TRAVAIL D'ÉTUDES ET DE RECHERCHE : NOMBRES CHANCEUX D'EULER ET FACTORIALITÉ

Ennio SALCICCIA
Encadré par Odile GAROTTA

Année 2024

Table des matières

Introduction

Notre histoire commence en 1772, lorsque Euler (1707-1783) écrit à Daniel Bernoulli, en réponse à un mémoire écrit en 1771 : "Cette progression 41, 43, 47, 53, 61, 71, 83, 97, 113, 131, etc. dont le terme général est 41+ x + x^2, est d'autant plus remarquable que les 40 premiers termes sont tous des nombres premiers". En effet, cela semble assez remarquable que le polynôme $P(k) = k^2 + k + 41$ fournisse successivement 40 nombres premiers. On pourrait penser à une simple coïncidence, nonobstant dans ce TER on propose une étude des nombres n tels que $P(k) = k^2 + k + n$ soit premier pour tout k entre 0 et $n-2$. Un tel n est appelé un nombre chanceux d'Euler (dénomination proposée par François le Lionnais). De son temps, Euler avait identifié 6 nombres chanceux d'Euler :

$$\boxed{2, 3, 5, 11, 17, 41.}$$

On propose dans ce TER de faire le lien entre les nombres chanceux d'Euler n et la factorialité de l'anneau des entiers de $\mathbb{Q}(i\sqrt{4n-1})$. Mais avant de pouvoir faire ce lien il faut d'abord comprendre ce qu'est l'anneau des entiers d'un corps quadratique. Ainsi dans un premier temps on introduit quelques outils théoriques comme les modules et les réseaux d'un espace euclidien en prouvant au passage le théorème de Minkowski sur l'existence de points proches de l'origine dans un réseau. Puis, on définit les anneaux de Dedekind ainsi que les anneaux d'entiers des corps quadratiques. Notre étude se déroule ensuite principalement dans les anneaux quadratiques imaginaires $\mathbb{Q}(i\sqrt{q})$, où l'on démontrera une version plus faible du théorème de Stark-Heegner (1967) :

$$\boxed{\text{Soit } q > 0 \text{ sans facteur carré alors } \mathcal{A}_q \text{ est principal si et seulement si } q \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}}$$

où $\mathcal{A}_q$ désigne l'anneau des entiers de $\mathbb{Q}(i\sqrt{q})$. On propose ici une démonstration pour $q < 10\ 000$. Enfin on clôture ce TER avec le théorème de Rabinowitsch :
Soit $n > 1$ tel que $4n - 1$ soit sans facteur carré alors :

$$\boxed{n \text{ est un nombre chanceux d'Euler si et seulement si } \mathcal{A}_{4n-1} \text{ est principal.}}$$

Faisant ainsi de $41 = \frac{163+1}{4}$ le plus grand nombre chanceux d'Euler.

« La mathématique est la reine des sciences et la théorie des nombres est la reine des mathématiques. » Gauss

Chapitre 1

Le matériel théorique

On considère qu'un corps est un anneau à division commutatif.

1.1 Préliminaires

1.1.1 Module à gauche, module à droite

Le but de cette sous-section est d'introduire la structure de $\mathcal{A}$-module, à savoir l'équivalent de la structure de $\mathcal{K}$-espace vectoriel mais pour des anneaux (commutatifs). Le lecteur à l'aise avec la théorie des modules peut sauter cette sous-section et la prochaine.

Définition 1.1.1 ($\mathcal{A}$-module à gauche)**.** *Soit $\mathcal{A}$ un anneau (dont la multiplication sera notée par simple juxtaposition), un $\mathcal{A}$-module à gauche est un triplet $(\mathcal{M}, +, \bullet)$ où :*
- $\mathcal{M}$ est un ensemble
- $+ : \mathcal{M} \times \mathcal{M} \to \mathcal{M}$ est une loi de composition interne sur $\mathcal{M}$
- $\bullet : \mathcal{A} \times \mathcal{M} \to \mathcal{M}$ est une loi de composition externe (à gauche) sur $\mathcal{M}$
tel que :
(i) $(\mathcal{M}, +)$ est un groupe abélien
(ii) $\forall a \in \mathcal{A},\ \forall (x, y) \in \mathcal{M}^2,\ a \bullet (x + y) = a \bullet x + a \bullet y$
(iii) $\forall (a, b) \in \mathcal{A}^2,\ \forall x \in \mathcal{M},\ (a + b) \bullet x = a \bullet x + b \bullet x$
(iv) $\forall x \in \mathcal{M},\ 1_{\mathcal{A}} \bullet x = x$
(v) $\forall (a, b) \in \mathcal{A}^2,\ \forall x \in \mathcal{M},\ (ab) \bullet x = a \bullet (b \bullet x)$.

Définition 1.1.2 ($\mathcal{A}$-module à droite)**.** *Avec les notations précédentes on définit un $\mathcal{A}$-module à droite en remplaçant (v) par :*
(v') $\forall (a, b) \in \mathcal{A}^2,\ \forall x \in \mathcal{M},\ (ab) \bullet x = b \bullet (a \bullet x)$.

Remarque 1.1.1. Ainsi même si on parle de $\mathcal{A}$-module à droite, la loi $\bullet$ reste une loi de composition externe à gauche.

Remarque 1.1.2. Dans la définition précédente on parle de distributivité de $\bullet$ sur l'addition de $\mathcal{M}$ pour (ii) et de distributivité de $\bullet$ sur l'addition de $\mathcal{A}$ pour (iii), pour le point (iii) on remarquera que le " $+$ " à droite de l'égalité fait référence à l'addition de $\mathcal{M}$, alors que le " $+$ " à gauche fait référence à l'addition de $\mathcal{A}$.

Remarque 1.1.3. Si $\mathcal{A}$ est un anneau commutatif, la notion de $\mathcal{A}$-module à gauche coïncide avec celle de $\mathcal{A}$-module à droite, c'est pourquoi, dans ce cas là on parlera simplement de "$\mathcal{A}$-module".

Remarque 1.1.4. Si $\mathcal{A}$ est un corps alors la notion de $\mathcal{A}$-module coïncide avec celle de $\mathcal{A}$-espace vectoriel.

Remarque 1.1.5. Dans la suite, on va se restreindre à des anneaux commutatifs, où il sera courant de noter $a \bullet x$ simplement ax car pour un $\mathcal{A}$-module à gauche on peut parler sans ambiguïté de abx.
En effet, on a :

$$a(bx) = a \bullet (bx) = a \bullet (b \bullet x) = (ab) \bullet x = (ab)x.$$

Remarque 1.1.6. Dans la suite, on commettra l'abus de langage d'identifier $(\mathcal{M}, +, \bullet)$ avec l'ensemble sous-jacent $\mathcal{M}$, ainsi on s'autorise à employer la terminologie : "Soit $\mathcal{M}$ un $\mathcal{A}$-module".

Proposition 1.1.1 (Règles de calcul)**.** *Soit $\mathcal{M}$ un $\mathcal{A}$-module (à gauche ou à droite) alors :*
$\forall a \in \mathcal{A},\ a \bullet 0_{\mathcal{M}} = 0_{\mathcal{M}}$
$\forall x \in \mathcal{M},\ 0_{\mathcal{A}} \bullet x = 0_{\mathcal{M}}$
$\forall x \in \mathcal{M},\ -x = (-1_{\mathcal{A}}) \bullet x.$

Démonstration. :
Soit $a \in \mathcal{A}$ et $x \in \mathcal{M}$ on remarque alors que :

$$0_{\mathcal{M}} = a \bullet 0_{\mathcal{M}} - a \bullet 0_{\mathcal{M}} = a \bullet (0_{\mathcal{M}} + 0_{\mathcal{M}}) - a \bullet 0_{\mathcal{M}} = a \bullet 0_{\mathcal{M}} + a \bullet 0_{\mathcal{M}} - a \bullet 0_{\mathcal{M}} = a \bullet 0_{\mathcal{M}}.$$

De la même manière on a :

$$0_{\mathcal{M}} = 0_{\mathcal{A}} \bullet x - 0_{\mathcal{A}} \bullet x = (0_{\mathcal{A}} + 0_{\mathcal{A}}) \bullet x - 0_{\mathcal{A}} \bullet x = 0_{\mathcal{A}} \bullet x + 0_{\mathcal{A}} \bullet x - 0_{\mathcal{A}} \bullet x = 0_{\mathcal{A}} \bullet x.$$

De plus :

$$x + (-1_{\mathcal{A}} \bullet x) = (1_{\mathcal{A}} \bullet x) + (-1_{\mathcal{A}} \bullet x) = (1_{\mathcal{A}} + (-1_{\mathcal{A}})) \bullet x = 0_{\mathcal{A}} \bullet x = 0_{\mathcal{M}}.$$

□

Les exemples qui suivent sont d'une importance capitale pour la suite.

Exemple 1.1.1. *Soit $(\mathcal{A}, +, \times)$ un anneau commutatif alors $\mathcal{A}$ est un $\mathcal{A}$-module pour $\bullet = \times$.*
Soit $\mathcal{B} \subset \mathcal{A}$ un sous-anneau de $\mathcal{A}$ alors $\mathcal{A}$ est un $\mathcal{B}$-module pour $\bullet : \mathcal{B} \times \mathcal{A} \to \mathcal{A}$, $(b, a) \mapsto b \times a$.
Soit $\mathcal{R}$ un anneau et $\mathcal{A}$ un sous-anneau de $\mathcal{R}$, soit $x \in \mathcal{R}$, alors :

$$\mathcal{A}[x] = \{P(x) \mid P \in \mathcal{A}[X]\}$$

est un sous-anneau de $\mathcal{R}$ contenant $\mathcal{A}$, en particulier c'est un $\mathcal{A}$-module.
En particulier, l'anneau des entiers de Gauβ, $\mathbb{Z}[i] = \{a + ib \mid (a, b) \in \mathbb{Z}^2\}$ est un $\mathbb{Z}$-module.

Exemple 1.1.2. *Soit $(\mathcal{G}, +)$ un groupe abélien noté additivement alors $\mathcal{G}$ est un $\mathbb{Z}$-module pour :*

$$\bullet : \mathbb{Z} \times \mathcal{G} \to \mathcal{G}$$

$$(n, g) \mapsto ng.$$

1.1.2 Sous-module, module de type fini

L'objectif est maintenant d'arriver à comprendre ce qu'est un $\mathcal{A}$-module de type fini.
Désormais et pour toute la suite on ne considère plus que des anneaux commutatifs sauf mention du contraire.

Définition 1.1.3 (Sous-module)**.** *Soit $\mathcal{M}$ un $\mathcal{A}$-module, et $\mathcal{N}$ une partie de $\mathcal{M}$, on dit que $\mathcal{N}$ est un sous-module de $\mathcal{M}$ si :*
(i) $(\mathcal{N}, +)$ est un sous-groupe de $(\mathcal{M}, +)$
(ii) $\forall a \in \mathcal{A},\ \forall x \in \mathcal{N},\ ax \in \mathcal{N}$.

Proposition 1.1.2 (Caractérisation des sous-modules)**.** *Avec les notations précédentes, $\mathcal{N}$ est un sous-*

module de $\mathcal{M}$ si et seulement si $\mathcal{N}$ est non vide et :

$$\forall (a,b) \in \mathcal{A}^2,\ \forall (x,y) \in \mathcal{N}^2,\ ax+by \in \mathcal{N}.\ (\spadesuit)$$

Démonstration. :
$\boxed{\Longrightarrow}$: Soit $\mathcal{N}$ un sous-module de $\mathcal{M}$, alors par (ii), $(ax, by) \in \mathcal{N}^2$ et par (i) on a que $\mathcal{N}$ est non vide et $\mathcal{N}$ est stable par $+$ donc $ax+by \in \mathcal{N}$.
$\boxed{\Longleftarrow}$: Soit $\mathcal{N} \subset \mathcal{M}$ non vide qui vérifie ($\spadesuit$) alors en prenant $a = 1_{\mathcal{A}}$ et $b = -1_{\mathcal{A}}$ on a que : $x - y \in \mathcal{N}$ donc $\mathcal{N}$ est un sous-groupe de $\mathcal{M}$. En prenant ensuite $a = 1_{\mathcal{A}}$ et $b = 0_{\mathcal{A}}$ on a que : $ax \in \mathcal{N}$ donc finalement $\mathcal{N}$ est un sous-module de $\mathcal{M}$. □

Remarque 1.1.7. Si $\mathcal{A}$ est un corps la notion de sous-module coïncide avec celle de sous-espace vectoriel.

Remarque 1.1.8. Si $\mathcal{N}$ est un sous-module de $\mathcal{M}$, alors $\mathcal{N}$ est un $\mathcal{A}$-module pour les lois induites.

Exemple 1.1.3. *Si on voit $\mathcal{A}$ comme un $\mathcal{A}$-module alors les sous-modules de $\mathcal{A}$ sont exactement les idéaux de $\mathcal{A}$.*

Exemple 1.1.4. *Les sous-modules triviaux $\{0_{\mathcal{M}}\}$ et $\mathcal{M}$ sont toujours des sous-modules de $\mathcal{M}$.*

Proposition 1.1.3 (Intersection quelconque de sous-modules)**.** *Soit $\mathcal{A}$ un anneau et $\mathcal{M}$ un $\mathcal{A}$-module, soit $(\mathcal{N}_i)_{i\in I}$ une famille (quelconque) de sous-modules de $\mathcal{M}$ alors $\bigcap_{i\in I}\mathcal{N}_i$ est un sous-module de $\mathcal{M}$.*

Démonstration. :
Une intersection quelconque de sous-groupes est un sous-groupe donc $\bigcap_{i\in I}\mathcal{N}_i$ est un sous-groupe de $\mathcal{M}$. Soit $(a,x) \in \mathcal{A} \times \bigcap_{i\in I}\mathcal{N}_i$ alors pour tout $i \in I$, $x \in \mathcal{N}_i$ or $\mathcal{N}_i$ est un sous-module donc pour tout $i \in I$, $ax \in \mathcal{N}_i$ donc $ax \in \bigcap_{i\in I}\mathcal{N}_i$. □

Définition 1.1.4 (Somme finie de sous-modules)**.** *Soit $\mathcal{A}$ un anneau et $\mathcal{M}$ un $\mathcal{A}$-module, soit $\mathcal{N}_1, ..., \mathcal{N}_n$ une famille finie de sous-modules de $\mathcal{M}$, on définit leur somme $\mathcal{S} = \sum_{i=1}^n \mathcal{N}_i$ comme étant l'ensemble des sommes d'éléments des $(\mathcal{N}_i)_{1\leq i\leq n}$:*

$$x \in \mathcal{S} \Longleftrightarrow \exists (x_1, ..., x_n) \in \mathcal{N}_1 \times ... \times \mathcal{N}_n,\ x = \sum_{i=1}^n x_i.$$

Proposition 1.1.4. *Avec les notations précédentes, $\mathcal{S}$ est un sous-module de $\mathcal{M}$.*

Démonstration. :
Pour tout $i \in [[1,n]]$, $0_{\mathcal{M}} \in \mathcal{N}_i$ (sous-groupe) donc $0_{\mathcal{M}} = \sum_{i=1}^n 0_{\mathcal{M}} \in \mathcal{S}$.
Soit $(x,y) \in \mathcal{S}^2$, soit alors $((x_1, ...x_n), (y_1, ..., y_n)) \in (\mathcal{N}_1 \times ... \times \mathcal{N}_n)^2$ tels que $x = \sum_{i=1}^n x_i$ et $y = \sum_{i=1}^n y_i$ alors $x - y = \sum_{i=1}^n (x_i - y_i)$ or, pour tout $i \in [[1,n]]$, $x_i - y_i \in \mathcal{N}_i$ (sous-groupe) donc $x - y \in \mathcal{S}$, donc $\mathcal{S}$ est un sous-groupe de $\mathcal{M}$.
Soit maintenant $a \in \mathcal{A}$ on a $ax = a\sum_{i=1}^n x_i = \sum_{i=1}^n ax_i$ or pour tout $i \in [[1,n]]$, $ax_i \in \mathcal{N}_i$ (sous-module) donc $ax \in \mathcal{S}$.

□

Définition 1.1.5 (Sous-module engendré définition de l'extérieur)**.** *Soit $\mathcal{M}$ un $\mathcal{A}$-module et $\mathcal{X}$ une partie de $\mathcal{M}$ alors l'intersection de tous les sous-modules de $\mathcal{M}$ contenant $\mathcal{X}$ reste un sous-module. C'est le plus petit sous-module de $\mathcal{M}$ (au sens de l'inclusion) contenant $\mathcal{X}$; on l'appelle sous-module engendré par $\mathcal{X}$ et on le note $< \mathcal{X} >$.*

Remarque 1.1.9. Dans le cas où $\mathcal{X} = \{x_1, ..., x_n\}$ est finie, on note simplement :

$$< \mathcal{X} >=< x_1, ..., x_n > .$$

Exemple 1.1.5. *Soit $\mathcal{R}$ un anneau et $\mathcal{A}$ un sous-anneau de $\mathcal{R}$, soit $x \in \mathcal{R}$ (on voit $\mathcal{R}$ comme un $\mathcal{A}$-module) alors $\mathcal{A}[x] =< \{x^k \mid k \in \mathbb{N}\} >$.*

Définition 1.1.6 (Combinaison linéaire)**.** *Soit $\mathcal{M}$ un $\mathcal{A}$-module et $(x_1, ..., x_n) \in \mathcal{M}^n$ une famille finie d'éléments de $\mathcal{M}$, soit également $z \in \mathcal{M}$, on dit que z est une combinaison linéaire des $(x_1, ..., x_n)$ s'il existe $(a_1, ..., a_n) \in \mathcal{A}^n$ tels que :*

$$z = \sum_{i=1}^{n} a_i x_i.$$

.

Définition 1.1.7 (Droite)**.** *Soit $\mathcal{M}$ un $\mathcal{A}$-module et $x \in \mathcal{M}$, on définit alors $\mathcal{A}x = \{ax \mid a \in \mathcal{A}\}$.*

Remarque 1.1.10. C'est un sous-module de $\mathcal{M}$ et de plus $< x >= \mathcal{A}x$.

Théorème 1.1.1 (Sous-module engendré définition de l'intérieur)**.** *Soit $\mathcal{M}$ un $\mathcal{A}$-module et $\mathcal{X} = \{x_1, ..., x_n\}$ une partie finie de $\mathcal{M}$ alors le sous-module engendré par $\mathcal{X}$ est exactement l'ensemble des combinaisons linéaires des $(x_1, ..., x_n)$.*
En d'autres termes :

$$< x_1, ..., x_n >= \sum_{i=1}^{n} \mathcal{A}x_i.$$

Démonstration. :
On sait par la proposition 1.1.4 que $\mathcal{S} = \sum_{i=1}^{n} \mathcal{A}x_i$ est un sous-module de $\mathcal{M}$, de plus on a pour tout $i \in [[1, n]]$, $x_i \in \mathcal{A}x_i \subset \mathcal{S}$ donc $\mathcal{X} \subset \mathcal{S}$.
Montrons que $\mathcal{S}$ est bien minimal pour l'inclusion, soit $\mathcal{N}$ un sous-module de $\mathcal{M}$ contenant $\mathcal{X}$, soit alors $(a_1, ..., a_n) \in \mathcal{A}^n$, comme $\mathcal{N}$ contient $\mathcal{X}$ on a pour tout $i \in [[1, n]]$, $x_i \in \mathcal{N}$ donc $a_i x_i \in \mathcal{N}$ (sous module) et donc $\sum_{i=1}^{n} a_i x_i \in \mathcal{N}$ (sous-groupe), en d'autres termes $\mathcal{S} \subset \mathcal{N}$. □

Définition 1.1.8 (Module de type fini)**.** *Soit $\mathcal{M}$ un $\mathcal{A}$-module on dit que $\mathcal{M}$ est de type fini s'il est engendré par une famille finie d'éléments, donc s'il existe $(x_1, ..., x_n) \in \mathcal{A}^n$ tels que :*

$$\mathcal{M} = \sum_{i=1}^{n} \mathcal{A}x_i.$$

Remarque 1.1.11. Avec les notations précédentes, on dira que $(x_1, ..., x_n)$ est $\mathcal{A}$-génératrice.

Définition 1.1.9 (Famille $\mathcal{A}$-libre)**.** *Soit $\mathcal{M}$ un $\mathcal{A}$-module et $(x_1, ..., x_n) \in \mathcal{M}^n$ une famille finie d'éléments de $\mathcal{M}$ on dit que $(x_1, ..., x_n)$ est $\mathcal{A}$-libre si :*

$$\forall (a_1, ..., a_n) \in \mathcal{A}^n, \ \sum_{i=1}^{n} a_i x_i = 0 \implies \forall i \in [[1, n]], \ a_i = 0.$$

Définition 1.1.10 (Base)**.** *Soit $\mathcal{M}$ un $\mathcal{A}$-module et $(x_1, ..., x_n) \in \mathcal{M}^n$ une famille finie d'éléments de $\mathcal{M}$ on dit que $(x_1, ..., x_n)$ est une $\mathcal{A}$-base de $\mathcal{M}$ si :*
i) $(x_1, ..., x_n)$ est $\mathcal{A}$-libre

ii) $\mathcal{M} =< x_1, ..., x_n >$. *($(x_1, ..., x_n)$ est $\mathcal{A}$-génératrice)*

Définition 1.1.11 (Module $\mathcal{A}$-libre)**.** *Soit $\mathcal{M}$ un $\mathcal{A}$-module, on dit qu'il est $\mathcal{A}$-libre s'il possède une $\mathcal{A}$-base.*

1.1.3 Déterminant des matrices à coefficients dans un anneau commutatif

On rappelle qu'on suppose tous les anneaux évoqués commutatifs sauf mention du contraire.
Cette sous-section existe dans le seul but de démontrer que la formule de la comatrice reste vraie dans un anneau commutatif quelconque. Le lecteur à l'aise avec cette formule peut sauter cette sous-section.

Définition 1.1.12 (Déterminant)**.** *Soit $\mathcal{A}$ un anneau et $M \in \mathcal{M}_n(\mathcal{A})$ une matrice carrée à coefficients dans $\mathcal{A}$ de taille $n \times n$, on définit le déterminant de $M = (m_{i,j})_{1 \leq i,j \leq n}$ par la formule de Leibniz :*

$$det(M) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} m_{\sigma(i),i}.$$

Remarque 1.1.12. Avec les notations précédentes, si M est de la forme $\begin{pmatrix} N & 0 \\ L & 1 \end{pmatrix}$ avec $N \in \mathcal{M}_{n-1}(\mathcal{A})$ alors : $\det(M) = \det(N)$.
En effet :

$$\det(M) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} m_{\sigma(i),i} = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma)(m_{\sigma(n),n}) \prod_{i=1}^{n-1} m_{\sigma(i),i} = \sum_{\substack{\sigma \in \mathfrak{S}_n \\ \sigma(n)=n}} \varepsilon(\sigma) \prod_{i=1}^{n-1} m_{\sigma(i),i}.$$

Or : $\varphi : \{\sigma \mid \sigma \in \mathfrak{S}_n, \sigma(n) = n\} \to \mathfrak{S}_{n-1}$, $\sigma \mapsto \sigma_{|[[1,n-1]]}$ est une bijection.
Donc :

$$\det(M) = \sum_{\sigma \in \mathfrak{S}_{n-1}} \varepsilon(\varphi^{-1}(\sigma)) \prod_{i=1}^{n-1} m_{\varphi^{-1}(\sigma)(i),i}$$

or pour tout $\sigma \in \mathfrak{S}_{n-1}$ on a $\varepsilon(\varphi^{-1}(\sigma)) = \varepsilon(\sigma)$ et pour tout $i \in [[1, n-1]]$, $\varphi^{-1}(\sigma)(i) = \sigma(i)$, et au final :

$$\det(M) = \sum_{\sigma \in \mathfrak{S}_{n-1}} \varepsilon(\sigma) \prod_{i=1}^{n-1} m_{\sigma(i),i} = \det(N).$$

On en déduit que le déterminant d'une matrice triangulaire inférieure est égal au produit de ses termes diagonaux.

Remarque 1.1.13. Une matrice carrée a le même déterminant que sa transposée : $\det(M) = \det(M^T)$.
(On part de la formule de Leibniz et on utilise le changement d'indice $\sigma \mapsto \sigma^{-1}$ pour la somme et le changement d'indice $i \mapsto \sigma(i)$ pour le produit.)

Pour la suite il sera commun de se référer à une matrice M en écrivant $M = \begin{pmatrix} C_1 & ... & C_j & ... & C_n \end{pmatrix}$ où les $(C_j)_{1 \leq j \leq n}$ sont les colonnes de M.

Théorème 1.1.2 (Propriétés du déterminant)**.** *L'application $det : \mathcal{M}_n(\mathcal{A}) \to \mathcal{A}, M \mapsto det(M)$ est :*
i) linéaire en les colonnes de M :
$det(\begin{pmatrix} C_1 & ... & A_j + \lambda B_j & ... & C_n \end{pmatrix}) = det(\begin{pmatrix} C_1 & ... & A_j & ... & C_n \end{pmatrix}) + \lambda det(\begin{pmatrix} C_1 & ... & B_j & ... & C_n \end{pmatrix})$.
ii) nulle si deux colonnes de M sont égales :
si $C_l = C_k$ (et $k \neq l$) alors $det(\begin{pmatrix} C_1 & ... & C_k & ... & C_l & ... & C_n \end{pmatrix}) = 0$.

Démonstration. :

i) : Soit $j \in [[1,n]]$ et $M = (m_{i,j})_{1\le i,j\le n} = \begin{pmatrix} C_1 & \dots & C_j & \dots & C_n \end{pmatrix}$ tel que : $C_j = A_j + \lambda B_j = \begin{pmatrix} a_{1,j} + \lambda b_{1,j} \\ \dots \\ a_{i,j} + \lambda b_{i,j} \\ \dots \\ a_{n,j} + \lambda b_{n,j} \end{pmatrix}$

alors on a :

$$\det(M) = \sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} m_{\sigma(i),i} = \sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma)(a_{\sigma(j),j} + \lambda b_{\sigma(j),j}) \prod_{\substack{i=1\\ i\neq j}}^{n} m_{\sigma(i),i}$$

$$= \sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma) a_{\sigma(j),j} \prod_{\substack{i=1\\ i\neq j}}^{n} m_{\sigma(i),i} + \lambda \sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma) b_{\sigma(j),j} \prod_{\substack{i=1\\ i\neq j}}^{n} m_{\sigma(i),i}$$

$$= \det(\begin{pmatrix} C_1 & \dots & A_j & \dots & C_n \end{pmatrix}) + \lambda \det(\begin{pmatrix} C_1 & \dots & B_j & \dots & C_n \end{pmatrix}).$$

ii) : Soit $M = \begin{pmatrix} C_1 & \dots & C_k & \dots & C_l & \dots & C_n \end{pmatrix}$ avec $C_l = C_k$ (et $k \neq l$), soit $\tau = (k\ l)$ la transposition de $\mathfrak{S}_n$ qui échange k et l. On remarque d'abord que : $\varphi : \mathfrak{A}_n \to \mathfrak{S}_n \setminus \mathfrak{A}_n$, $\sigma \mapsto \tau \circ \sigma$ est une bijection. Donc :

$$\det(M) = \det(M^T) = \sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} m_{i,\sigma(i)} = \sum_{\sigma\in\mathfrak{A}_n} \prod_{i=1}^{n} m_{i,\sigma(i)} - \sum_{\sigma\in\mathfrak{S}_n\setminus\mathfrak{A}_n} \prod_{i=1}^{n} m_{i,\sigma(i)}$$

$$= \sum_{\sigma\in\mathfrak{A}_n} \prod_{i=1}^{n} m_{i,\sigma(i)} - \sum_{\sigma\in\mathfrak{A}_n} \prod_{i=1}^{n} m_{i,(\tau\circ\sigma)(i)}$$

$$= \sum_{\sigma\in\mathfrak{A}_n} (\prod_{i=1}^{n} m_{i,\sigma(i)} - \prod_{i=1}^{n} m_{i,(\tau\circ\sigma)(i)}) = 0.$$

□

Corollaire 1.1.1. *Si l'on échange deux colonnes d'une matrice, cela multiplie son déterminant par -1. Si l'on échange deux lignes d'une matrice, cela multiplie son déterminant par -1.*

Définition 1.1.13 (Cofacteur)**.** *Soit $M \in \mathcal{M}_n(\mathcal{A})$, soit $(i,j) \in [[1,n]]^2$, on définit le cofacteur d'indice i,j de M comme suit :*

$$com(M)_{i,j} = det(M'_{i,j}) = (-1)^{i+j} det(M_{i,j})$$

Où $M'_{i,j}$ est la matrice carrée de taille n déduite de M en remplacant la j-ième colonne par une colonne constituée uniquement de zéros, sauf un 1 sur la i-ième ligne.
Où $M_{i,j}$ est la sous-matrice carrée de taille $n-1$ déduite de M en supprimant la i-ième ligne et la j-ième colonne.

Remarque 1.1.14. [Preuve que les définitions sont équivalentes] Pour calculer $\det(M'_{i,j})$ on effectue des transpositions successives sur ses colonnes : $(j\ j+1), (j+1\ j+2), ..., (n-1\ n)$ puis on effectue sur ses lignes des transpositions : $(i\ i+1), (i+1\ i+2), ..., (n-1\ n)$ on a donc effectué $(n-j)+(n-i) = 2n-(i+j)$ transpositions pour se ramener à une matrice de la forme :

$$N = \begin{pmatrix} M_{i,j} & 0 \\ L & 1 \end{pmatrix}.$$

D'où la formule : $\det(M'_{i,j}) = (-1)^{2n-(i+j)} \det(N) = (-1)^{i+j} \det(M_{i,j})$.

Définition 1.1.14 (Comatrice)**.** *Soit $M \in \mathcal{M}_n(\mathcal{A})$, on définit la comatrice de M :*

$$com(M) = (com(M)_{i,j})_{1\le i,j\le n}.$$

Remarque 1.1.15. Soit $M \in \mathcal{M}_n(\mathcal{A})$ alors $com(M^T) = com(M)^T$.

Proposition 1.1.5 (Formule de Laplace). *Soit $M \in \mathcal{M}_n(\mathcal{A})$ alors on a les formules de développement du déterminant suivantes.*
Par rapport à la colonne j :

$$det(M) = \sum_{i=1}^{n} m_{i,j} com(M)_{i,j}.$$

Par rapport à la ligne i :

$$det(M) = \sum_{j=1}^{n} m_{i,j} com(M)_{i,j}.$$

Démonstration. :
Avec les notations précédentes et par linéarité du det par rapport à la j-ième colonne on a :

$$\det(M) = \sum_{i=1}^{n} m_{i,j} \det(M'_{i,j}).$$

Le développement par rapport à la ligne i, se déduit de celui par rapport à la ligne j avec M^T.

□

Théorème 1.1.3 (Formule de la comatrice). *Soit $M \in \mathcal{M}_n(\mathcal{A})$ alors on a :*

$$M com(M)^T = com(M)^T M = det(M) I_n.$$

Démonstration. :
Par transposition, il suffit de montrer une des deux égalités, montrons par exemple : $\mathrm{com}(M)^T M = \det(M) I_n$. D'après le développement du déterminant par rapport à la colonne j on a l'égalité des termes diagonaux de ces deux matrices :

$$[\mathrm{com}(M)^T M]_{j,j} = \sum_{i=1}^{n} \mathrm{com}(M)_{i,j} m_{i,j} = \det(M) = [\det(M) I_n]_{j,j}.$$

Il reste à prouver que pour $k \neq j$, $[\mathrm{com}(M)^T M]_{j,k} = 0$ or :

$$[\mathrm{com}(M)^T M]_{j,k} = \sum_{i=1}^{n} (\mathrm{com}(M))_{i,j} m_{i,k}$$

mais toujours par le développement du déterminant par rapport à la colonne j, cette somme est égale au déterminant de la matrice M en remplacant la j-ième colonne par la k-ième. Comme la matrice obtenue a deux colonnes égales, son déterminant est nul.

□

1.2 Réseaux d'un espace euclidien

Pour tout $x \in \mathbb{R}$ on note $\lfloor x \rfloor$ sa partie entière et $\{x\} = x - \lfloor x \rfloor$ sa partie fractionnaire. Pour toute cette section n désigne un entier ≥ 1. Toutes les normes sur $\mathbb{R}^n$ étant équivalentes on n'en précisera aucune sauf si besoin. Pour toute la suite, on parlera du déterminant d'une famille de vecteurs sans préciser qu'on prend comme base de référence la base canonique, ainsi on parlera simplement de $\det(v_1, ..., v_n)$ $(v_i \in \mathbb{R}^n)$.
Le but des trois prochaines sous-sections est de démontrer le théorème de Minkowski pour les réseaux, ce théorème est très utile en arithmétique et nous servira grandement pour le chapitre 2. Il s'agit d'un théorème qui affirme l'existence de points proches de 0 dans un réseau.

1.2.1 Définition et caractérisation des réseaux

Définition 1.2.1 (Point isolé)**.** *Soit E un espace métrique et $\Lambda \subset E$ non vide et $\lambda \in \Lambda$, on dit que λ est isolé dans Λ s'il existe $r > 0$ tel que :*

$$B(\lambda, r) \cap \Lambda = \{\lambda\}.$$

Remarque 1.2.1. Une définition équivalente est que toute suite de Λ qui converge vers λ est stationnaire (et stationne en λ).

Définition 1.2.2 (Partie discrète)**.** *Soit E un espace métrique et $\Lambda \subset E$ non vide, on dit que Λ est discret si tous les éléments de Λ sont isolés dans Λ.*

Proposition 1.2.1. *Soit E un espace vectoriel normé de dimension finie et $\Lambda \subset E$. Alors les assertions suivantes sont équivalentes :*
i) Pour tout $x \in E$, il existe $r > 0$ tel que $\Lambda \cap B(x, r)$ soit fini
ii) Pour tout compact $\mathcal{K} \subset E$, $\mathcal{K} \cap \Lambda$ est fini
iii) Λ est une partie discrète et fermée.

Démonstration. :
i) $\implies$ ii) : Soit $\mathcal{K} \subset E$ compact alors par hypothèse pour tout $x \in \mathcal{K}$ il existe $r_x > 0$ tel que $\Lambda \cap B(x, r_x)$ soit fini. Ainsi :

$$\mathcal{K} \subset \bigcup_{x \in \mathcal{K}} B(x, r_x)$$

et on peut donc extraire un sous-recouvrement fini de ce recouvrement par des ouverts (car $\mathcal{K}$ est compact), soit donc $N \in \mathbb{N}$ et $x_1, ..., x_N \in \mathcal{K}$ tels que :

$$\mathcal{K} \subset \bigcup_{i=1}^{N} B(x_i, r_{x_i}).$$

On obtient alors :

$$\mathcal{K} \cap \Lambda \subset \bigcup_{i=1}^{N} (B(x_i, r_{x_i}) \cap \Lambda)$$

le membre de droite étant une union finie d'ensembles finis il est fini et donc $\mathcal{K} \cap \Lambda$ est fini.
ii) $\implies$ iii) : Soit $\lambda \in \Lambda$, la boule $\overline{B}(\lambda, 1)$ étant compacte on a que $\overline{B}(\lambda, 1) \cap \Lambda$ est fini, si cette intersection est réduite à $\{\lambda\}$ alors λ est isolé dans Λ sinon on note $x_1, ..., x_N$ $(N \geq 1)$ les éléments de $\overline{B}(\lambda, 1) \cap \Lambda$ distincts de λ et considérons :

$$A = \{d(\lambda, x_i) \mid i \in [[1, N]]\}$$

alors A est non vide et fini donc il admet un plus petit élément $r > 0$ (on ne peut pas avoir $r = 0$ car les x_i sont distincts de λ) et alors $B(\lambda, \frac{r}{2}) \cap \Lambda = \{\lambda\}$. Donc Λ est une partie discrète.
Montrons qu'elle est fermée : soit $x \in \overline{\Lambda}$, par l'absurde supposons que $x \notin \Lambda$ soit alors une suite injective $(x_n)_{n \in \mathbb{N}} \in \Lambda^{\mathbb{N}}$ tel que $x_n \to x$. (On peut supposer la suite injective car $x \notin \Lambda$) mais alors $\overline{B}(x, 1) \cap \Lambda$ contient une infinité de termes de la suite, c'est une contradiction avec ii).
iii) $\implies$ i) : Soit $x \in E$ si $x \in \Lambda^c$ celui-ci étant ouvert il existe $r > 0$ tel que $B(x, r) \cap \Lambda = \emptyset$ et l'intersection est a fortiori finie. Si $x \in \Lambda$ il est isolé dans Λ et on obtient bien la conclusion cherchée. □

Exemple 1.2.1. *$\mathbb{Z}^n$ est une partie discrète de $\mathbb{R}^n$.*
$\mathbb{Q}$ n'est pas une partie discrète de $\mathbb{R}$.
$\{\frac{1}{n} \mid n \in \mathbb{N}^*\}$ est une partie discrète de $\mathbb{R}$.
$\{\frac{1}{n} \mid n \in \mathbb{N}^*\} \cup \{0\}$ n'est pas une partie discrète de $\mathbb{R}$.

Proposition 1.2.2. *Soit $\mathcal{G} \subset \mathbb{R}^n$ un sous-groupe additif discret alors $\mathcal{G}$ est fermé.*

Démonstration. :
Soit $(g_n)_{n\in\mathbb{N}} \in \mathcal{G}^{\mathbb{N}}$ une suite convergente qui converge vers $g \in \mathbb{R}^n$. Par convergence de la suite $(g_n)_{n\in\mathbb{N}}$ la suite $(g_{n+1} - g_n)_{n\in\mathbb{N}}$ converge et elle converge vers 0 mais $0 \in \mathcal{G}$ (sous-groupe additif) et de même pour tout $n \in \mathbb{N},\ g_{n+1} - g_n \in \mathcal{G}$. Ainsi comme $\mathcal{G}$ est discret la suite $(g_{n+1} - g_n)_{n\in\mathbb{N}}$ est stationnaire et stationne vers 0 (remarque 16) autrement dit, la suite $(g_n)_{n\in\mathbb{N}}$ est stationnaire et donc $g \in \mathcal{G}$ et par conséquent $\mathcal{G}$ est fermé. □

Définition 1.2.3 (Réseau)**.** *Un réseau de $\mathbb{R}^n$ est une partie $\Lambda \subset \mathbb{R}^n$ telle que :*
i) $(\Lambda, +)$ est un sous-groupe de $(\mathbb{R}^n, +)$
ii) Λ est une partie discrète de $\mathbb{R}^n$
iii) $Vect(\Lambda) = \mathbb{R}^n$.

Remarque 1.2.2. En combinant les propositions 1.2.1 et 1.2.2, étant donné $\Lambda \subset \mathbb{R}^n$ un sous-groupe additif de $\mathbb{R}^n$ il y a équivalence entre :
i) Pour tout compact $\mathcal{K} \subset \mathbb{R}^n,\ \mathcal{K} \cap \Lambda$ est fini
ii) Λ est un sous-groupe discret.

Remarque 1.2.3. De plus, on peut remplacer i) Pour tout compact $\mathcal{K} \subset \mathbb{R}^n,\ \mathcal{K} \cap \Lambda$ est fini par l'une des deux propriétés suivantes équivalentes :
i') Pour toute partie $\mathcal{K}$ bornée $\subset \mathbb{R}^n,\ \mathcal{K} \cap \Lambda$ est fini
i") Pour tout $r > 0,\ B(0, r) \cap \Lambda$ est fini.

Remarque 1.2.4. Dans la remarque précédente on parle de boule sans préciser de norme sur $\mathbb{R}^n$ car les normes étant toutes équivalentes, la notion de "bornée" ou de "compacte" ne dépend que de la partie considérée. (si une partie est bornée / compacte pour une norme alors elle l'est pour toutes les normes.) C'est pourquoi on définit dans la suite une norme qui s'avérera pratique.

Remarque 1.2.5. Étant donnée $e = (e_1, ..., e_n)$ une $\mathbb{R}$-base de $\mathbb{R}^n$, on note : $||\ ||_e : \mathbb{R}^n \to \mathbb{R}$, $v = \sum_{i=1}^n v_i e_i \mapsto max\{|v_i| \mid i \in [[1, n]]\}$ la norme associée à e.
On note également pour tout $r > 0 : B_e(0, r) = \{v \in \mathbb{R}^n \mid ||v||_e < r\}$.

Pour toute la suite, étant donné $e = (e_1, ..., e_n)$ une $\mathbb{R}$-base $\mathbb{R}^n$ et $A \subset \mathbb{R}^n$, on s'autorise à écrire $e \subset A$ pour désigner que pour tout $i \in [[1, n]],\ e_i \in A$.

Définition 1.2.4. *Soit $e = (e_1, ..., e_n)$ une $\mathbb{R}$-base de $\mathbb{R}^n$, on note :*

$$\Lambda(e) =< e_1, ..., e_n >= \sum_{i=1}^{n} \mathbb{Z} e_i$$

le sous-$\mathbb{Z}$-module de $\mathbb{R}^n$ (vu comme un $\mathbb{Z}$-module) engendré par e.

Proposition 1.2.3. *Avec les notations précédentes, $\Lambda(e)$ est un réseau de $\mathbb{R}^n$.*

Démonstration. :
$\Lambda(e)$ est un sous-$\mathbb{Z}$-module de $\mathbb{R}^n$ donc c'est un sous-groupe de $(\mathbb{R}^n, +)$. Le fait que $e \subset \Lambda(e)$ assure que $Vect(\Lambda(e)) = \mathbb{R}^n$. De plus, il apparaît clairement que $|\Lambda(e) \cap B_e(0, r)| \leq \lfloor 2r + 1 \rfloor^n$ et obtient ainsi le caractère discret (remarque 1.2.3). □

Définition 1.2.5 (Pavé fondamental). *Soit $e = (e_1, ..., e_n)$ une $\mathbb{R}$-base de $\mathbb{R}^n$, on définit le pavé fondamental de $\mathbb{R}^n$ associé à e et on note $P(e)$ l'ensemble suivant :*

$$P(e) = \{\sum_{i=1}^{n} \theta_i e_i \mid (\theta_1, ..., \theta_n) \in [0,1[^n\}.$$

Lemme 1.2.1. *Soit $e = (e_1, ..., e_n)$ une $\mathbb{R}$-base de $\mathbb{R}^n$, alors :*

$$\forall v \in \mathbb{R}^n,\ \exists!(\lambda(v), \theta(v)) \in \Lambda(e) \times P(e),\ v = \lambda(v) + \theta(v).$$

Démonstration. :
Si $v = \sum_{i=1}^n v_i e_i$, il est clair que poser : $\theta(v) = \sum_{i=1}^n \{v_i\} e_i$ et $\lambda(v) = \sum_{i=1}^n \lfloor v_i \rfloor e_i$ fournit une décomposition qui convient. Montrons que c'est la seule : soit $\lambda'(v)$ et $\theta'(v)$ une décomposition qui vérifie l'énoncé, e étant une base de $\mathbb{R}^n$ on a nécessairement que pour tout $i \in [[1, n]]$: $v_i = \lambda'_i + \theta'_i$ autrement dit : $v_i - \lambda'_i = \theta'_i \in [0, 1[$ et donc par unicité de la partie entière : $\lambda'_i = \lfloor v_i \rfloor$ et le reste s'en déduit. □

Lemme 1.2.2. *Soit Λ un réseau de $\mathbb{R}^n$ et $e = (e_1, ..., e_n)$ une $\mathbb{R}$-base de $\mathbb{R}^n$ telle que $e \subset \Lambda$. Alors $\Lambda(e)$ est un sous-groupe de Λ et :*
i) $\Lambda(e)$ est d'indice fini dans Λ
ii) $\Lambda \subset \frac{1}{[\Lambda:\Lambda(e)]}\Lambda(e)$. (où $[\Lambda : \Lambda(e)]$ est l'indice de $\Lambda(e)$ dans Λ)

Démonstration. :
Comme $e \subset \Lambda$ a fortiori $< e >= \Lambda(e)$ est un sous-$\mathbb{Z}$-module de Λ.
De plus, l'application

$$\varphi : \Lambda \cap P(e) \to \Lambda/\Lambda(e)$$
$$x \mapsto \overline{x}$$

est surjective. ($\overline{x}$ désigne la classe de x modulo $\Lambda(e)$)
En effet, soit $\overline{v} \in \Lambda/\Lambda(e)$ alors comme $v = \theta(v) + \lambda(v)$ (ou $(\lambda(v), \theta(v))$ est une décomposition fournie par le lemme 1.2.1) on a aussi $\overline{v} = \overline{\theta(v)}$ et $\theta(v) = v - \lambda(v) \in \Lambda \cap P(e)$. D'où : $|\Lambda/\Lambda(e)| \leq |\Lambda \cap P(e)|$.
Mais $P(e)$ est borné (pour $||\ ||_e$ par exemple) donc $\Lambda \cap P(e)$ est fini, ainsi $\Lambda(e)$ est d'indice fini dans Λ.
Si on note $N = [\Lambda : \Lambda(e)]$ on sait alors par le théorème de Lagrange que pour tout $v \in \Lambda$, $N\overline{v} = \overline{Nv} = \overline{0}$, donc $Nv \in \Lambda(e)$ autrement dit : $\Lambda \subset \frac{1}{N}\Lambda(e)$. □

Proposition 1.2.4. *Soit Λ un réseau de $\mathbb{R}^n$ et soit :*

$$\mathfrak{B} = \{e \subset \Lambda \mid e \text{ est une } \mathbb{R}\text{-base de } \mathbb{R}^n\}$$

alors il existe $e = (e_1, ..., e_n) \in \mathfrak{B}$ telle que :

$$|det(e_1, ..., e_n)| \text{ est minimal et } \Lambda = \Lambda(e).$$

Démonstration. :
Comme $Vect(\Lambda) = \mathbb{R}^n$ on a par le théorème de la base extraite que $\mathfrak{B}$ est non vide, fixons $e \in \mathfrak{B}$.
Soit $f = (f_1, ..., f_n) \in \mathfrak{B}$ alors par le lemme précédent : $f \subset \Lambda \subset [\Lambda : \Lambda(e)]^{-1}\Lambda(e)$. Donc pour tout $i \in [[1, n]]$ il existe $(m_{i,j})_{j\in[[1,n]]}$ tel que : $f_i = \sum_{j=1}^n \frac{m_{i,j}}{[\Lambda:\Lambda(e)]} e_j$. En conséquence par multilinéarité du déterminant : $\det(f) \in [\Lambda : \Lambda(e)]^{-n}\det(e)\mathbb{Z}$.
L'ensemble $[\Lambda : \Lambda(e)]^{-n}\det(e)\mathbb{Z}$ est discret dans $\mathbb{R}$, on peut donc choisir $e_0 \in \mathfrak{B}$ tel que $|\det(e_0)|$ soit minimal (et comme e_0 est une base $\det(e_0) \neq 0$). Montrons maintenant que $\Lambda \subset \Lambda(e_0)$ avec $e_0 = (e_1, ..., e_n)$.
Pour cela on montre que $\Lambda \cap P(e_0) = \{0\}$ et le lemme 1.2.1 permettra alors de conclure. En effet, si $v \in \Lambda$ alors on peut écrire $v = \lambda(v) + \theta(v)$ mais alors $\theta(v) = v - \lambda(v) \in \Lambda \cap P(e_0)$ et donc $\theta(v) = 0$ et $v = \lambda(v) \in \Lambda(e_0)$.
Soit $\theta = \sum_{i=1}^n \theta_i e_i \in \Lambda \cap P(e_0)$ supposons qu'il existe $i \in [[1, n]]$ tel que $\theta_i \neq 0$ alors toujours par multilinéarité du déterminant :

$$0 < |\det(e_1, ..., e_{i-1}, \theta, e_{i+1}, ..., e_n)| = \theta_i |\det(e_1, ..., e_n)| < |\det(e_1, ..., e_n)|$$

contredisant alors la minimalité de $|\det(e_0)|$. □

Théorème 1.2.1 (Caractérisation algébrique des réseaux). *Soit $\Lambda \subset \mathbb{R}^n$ un sous-groupe de $(\mathbb{R}^n, +)$. Alors les assertions suivantes sont équivalentes :*
i) Λ est un réseau de $\mathbb{R}^n$
ii) Λ admet une famille $\mathbb{Z}$-génératrice qui est une $\mathbb{R}$-base de $\mathbb{R}^n$.

Démonstration. :
ii) $\implies$ i) : c'est la proposition 1.2.3.
i) $\implies$ ii) : c'est la proposition 1.2.4. □

Remarque 1.2.6. En particulier, tout réseau de $\mathbb{R}^n$ admet une $\mathbb{Z}$-base de cardinal n.

1.2.2 Description des bases d'un réseau

Proposition 1.2.5 (Caractérisation des $\mathbb{Z}$-bases d'un réseau). *Soit Λ un réseau de $\mathbb{R}^n$ et $e = (e_1, ..., e_m)$ une famille $\mathbb{Z}$-génératrice de Λ ; alors $m \geq n$ et de plus les assertions suivantes sont équivalentes :*
i) e est une $\mathbb{Z}$-base de Λ
ii) e est une $\mathbb{R}$-base de $\mathbb{R}^n$
iii) $m = n$.

Démonstration. :
Soit $v \in \mathbb{R}^n$ alors v est une combinaison linéaire d'éléments de Λ (car $Vect(\Lambda) = \mathbb{R}^n$) donc en particulier v est une combinaison linéaire d'éléments de e donc e est une famille $\mathbb{R}$-génératrice de $\mathbb{R}^n$ donc $m \geq n$.
ii) $\iff$ iii) : C'est connu.
ii) $\implies$ i) : Une famille $\mathbb{R}$-libre est en particulier $\mathbb{Z}$-libre.
i) $\implies$ iii) : Soit :

$$\psi : \mathbb{Z}^m \to \Lambda$$
$$(m_i)_{1 \leq i \leq m} \mapsto \sum_{i=1}^{m} m_i e_i$$

alors ψ est un isomorphisme de groupes. Soit f une $\mathbb{Z}$-base de Λ à n éléments (remarque 1.2.6), alors $\psi^{-1}(f)$ est une $\mathbb{Z}$-base de $\mathbb{Z}^m$ à n éléments. Mais $\mathbb{Z}^m$ est naturellement un réseau de $\mathbb{R}^m$ donc $n \geq m$ par ce qui précède et donc $n = m$. □

Définition 1.2.6 ($GL_n(\mathbb{Z})$). *On note $GL_n(\mathbb{Z})$ le sous-groupe de $GL_n(\mathbb{R})$ constitué des matrices à coefficients entiers, et dont l'inverse est aussi à coefficients entiers.*
Autrement dit :

$$GL_n(\mathbb{Z}) = \{M \in \mathcal{M}_n(\mathbb{Z}) \mid \exists N \in \mathcal{M}_n(\mathbb{Z}),\ MN = NM = I_n\}.$$

Proposition 1.2.6 (Caractérisation de $GL_n(\mathbb{Z})$). *Soit $M \in \mathcal{M}_n(\mathbb{Z})$ alors :*

$$M \in GL_n(\mathbb{Z}) \iff det(M) = \pm 1.$$

Démonstration. :
$\implies$: Soit $N \in \mathcal{M}_n(\mathbb{Z})$ tel que $MN = I_n$ alors $(\det(M), \det(N)) \in \mathbb{Z}^2$ et :

$$\det(MN) = \det(M)\det(N) = \det(I_n) = 1$$

donc $\det(M) \in \mathbb{Z}^\times = \{\pm 1\}$.
$\impliedby$: Si $\det(M) \in \mathbb{Z}^\times$ alors la formule de la comatrice (théorème 1.1.3) nous fournit un inverse pour M :

$$N = (\det(M))^{-1} com(M)^T \in \mathcal{M}_n(\mathbb{Z})$$

□

Définition 1.2.7 (Matrice de passage). *Soit $e = (e_1, ..., e_n)$ et $f = (f_1, ..., f_n)$ deux $\mathbb{R}$-bases de $\mathbb{R}^n$ on note $P(e, f)$ la matrice de passage de e à f. Donc $f_j = \sum_{i=1}^{n} P(e, f)_{i,j} e_i$. (pour tous j)*

Remarque 1.2.7. Avec les notations précédentes, on rappelle le résultat : soit $v \in \mathbb{R}^n$, $X = (x_1, ..., x_n)$ ses coordonnées dans la base e et $Y = (y_1, ..., y_n)$ ses coordonnées dans la base f alors : $X^T = P(e, f)Y^T$.

Proposition 1.2.7. *Soit $e = (e_1, ..., e_n)$ et $f = (f_1, ..., f_n)$ deux $\mathbb{R}$-bases de $\mathbb{R}^n$ alors :*

$$\Lambda(e) = \Lambda(f) \iff P(e, f) \in GL_n(\mathbb{Z}).$$

Démonstration. :
On a :

$$P(e, f)P(f, e) = I_n. \ (\clubsuit)$$

Or par définition de $P(e, f)$ on a $f_j \in \Lambda(e)$ si et seulement si la j-ème colonne de $P(e, f)$ est à coefficients entiers donc :

$$\Lambda(f) \subset \Lambda(e) \iff P(e, f) \in \mathcal{M}_n(\mathbb{Z}).$$

Par symétrie des rôles de e et f et ($\clubsuit$) on a l'équivalence souhaitée. □

1.2.3 Théorème de Minkowski

Pour la suite on note μ la mesure de Lebesgue sur $\mathbb{R}^n$ et on suppose connue la théorie de la mesure et la formule générale de changement de variables.
Si $A \subset \mathbb{R}^n$ et $v \in \mathbb{R}^n$ on note $A + v = \{a + v \mid a \in A\}$. De même $A - v = A + (-v)$.
On rappelle que la mesure de Lebesgue est invariante par translation : $\mu(A) = \mu(A + v)$.

Définition 1.2.8 (domaine fondamental). *Soit Λ un réseau de $\mathbb{R}^n$ et $X \subset \mathbb{R}^n$ mesurable. On dit que X est un domaine fondamental de Λ si :*

$$\forall v \in \mathbb{R}^n, \ \exists!(\lambda, x) \in \Lambda \times X, \ v = \lambda + x.$$

Exemple 1.2.2. *Soit $e = (e_1, ..., e_n)$ une $\mathbb{R}$-base de $\mathbb{R}^n$ alors $P(e)$ est un domaine fondamental de $\Lambda(e)$ (lemme 1.2.1). De plus, il est de mesure $|det(e_1, ..., e_n)|$.*
En effet :

$$\mu(P(e)) = \int_{P(e)} 1 d\mu = \int_{P(e)\setminus\{0\}} 1 d\mu.$$

Or si on note b la base canonique de $\mathbb{R}^n$ on a que :

$$\varphi :]0, 1[^n \to P(e) \setminus \{0\}$$

$$(\theta_1, ..., \theta_n) \mapsto \sum_{i=1}^{n} \theta_i e_i = [P(b, e)(\theta_1 \ ... \ \theta_n)^T]^T$$

est un $\mathcal{C}^1$-difféomorphisme (restriction d'un isomorphisme linéaire) et pour tout $u \in]0, 1[^n$ on a :

$$J_\varphi(u) = P(b, e) = (e_1 \mid ... \mid e_n).$$

Donc par changement de variables :

$$\int_{P(e)\setminus\{0\}} 1 d\mu = \int_{]0,1[^n} |det(J_\varphi(u))| du = |det(e_1, ..., e_n)| \mu(]0, 1[^n) = |det(e_1, ..., e_n)|.$$

Proposition 1.2.8. *Tous les pavés fondamentaux d'un même réseau Λ ont la même mesure.*

Démonstration. :
Soit e et f deux $\mathbb{R}$-bases de $\mathbb{R}^n$ telles que : $\Lambda = \Lambda(e) = \Lambda(f)$. On a alors $P(e,f) \in GL_n(\mathbb{Z})$ (proposition 1.2.7) mais :

$$(f_1 \mid ... \mid f_n) = (e_1 \mid ... \mid e_n)P(e,f)$$

donc :

$$\mu(P(f)) = |\det((f_1 \mid ... \mid f_n))| = |\det((e_1 \mid ... \mid e_n))||\det(P(e,f))|$$

mais comme $P(e,f) \in GL_n(\mathbb{Z})$ nécessairement $|\det(P(e,f))| = 1$ et : $\mu(P(f)) = \mu(P(e))$. □

Théorème 1.2.2 (Théorème de Blichfeldt)**.** *Soit Λ un réseau de $\mathbb{R}^n$, X et Y deux parties de $\mathbb{R}^n$ mesurables. On suppose que X est un domaine fondamental de Λ et que Y vérifie la propriété suivante :*

$$\forall (x,y) \in Y^2,\ x - y \in \Lambda \implies x = y.$$

Alors $\mu(Y) \leq \mu(X)$.

Remarque 1.2.8. Il s'agit d'une version plus forte de la proposition 1.2.8. On déduit en particulier du théorème de Blichfeldt que tous les domaines fondamentaux d'un même réseau Λ ont le même volume.

Démonstration. :
Du fait que X est un domaine fondamental de Λ on a la décomposition suivante : $\mathbb{R}^n = \coprod_{\lambda \in \Lambda}(\lambda + X)$. Donc :

$$Y = \coprod_{\lambda \in \Lambda} Y \cap (\lambda + X)$$

ainsi comme $\mu(Y \cap (\lambda + X)) = \mu((Y \cap (\lambda + X)) - \lambda) = \mu((Y - \lambda) \cap X)$ on a :

$$\mu(Y) = \sum_{\lambda \in \Lambda} \mu((Y - \lambda) \cap X).$$

Or l'hypothèse faite sur Y assure que les ensembles $(Y - \lambda)_{\lambda \in \Lambda}$ sont disjoints et comme :

$$\coprod_{\lambda \in \Lambda} ((Y - \lambda) \cap X) \subset X.$$

On a finalement :

$$\sum_{\lambda \in \Lambda} \mu((Y - \lambda) \cap X) \leq \mu(X)$$

et $\mu(Y) \leq \mu(X)$. □

Définition 1.2.9 (Covolume d'un réseau)**.** *Le covolume d'un réseau Λ noté covol(Λ) est la mesure commune de ses domaines fondamentaux.*

Définition 1.2.10 (Convexe)**.** *Soit $C \subset \mathbb{R}^n$ on dit que C est convexe si :*

$$\forall (x,y) \in C^2,\ \forall t \in [0,1],\ tx + (1-t)y \in C.$$

Définition 1.2.11 (Partie symétrique)**.** *Soit $C \subset \mathbb{R}^n$ on dit que C est symétrique si :*

$$\forall x \in C,\ -x \in C.$$

Remarque 1.2.9. Si $C \subset \mathbb{R}^n$ est une partie convexe symétrique et $(x,y) \in C^2$ alors : $\frac{x-y}{2} = \frac{1}{2}x + \frac{1}{2}(-y) \in C$.

Théorème 1.2.3 (Théorème de Minkowski)**.** *Soit $C \subset \mathbb{R}^n$ une partie mesurable convexe symétrique et*

soit Λ un réseau de $\mathbb{R}^n$ si :

$$covol(\Lambda) < \frac{\mu(C)}{2^n}.$$

Alors, il existe un élément non nul dans $\Lambda \cap C$.
Si on suppose en plus que C est compacte alors on a une version plus forte du théorème en remplaçant l'inégalité stricte par une inégalité large.

Démonstration. :
Soit $\Lambda' = 2\Lambda \subset \Lambda$, alors Λ' est un réseau de $\mathbb{R}^n$. En effet, si e est une famille $\mathbb{Z}$-génératrice de Λ alors $2e$ est une famille $\mathbb{Z}$-génératrice de Λ'.
De plus $\det((2e_1 \mid ... \mid 2e_n)) = 2^n \det((e_1 \mid ... \mid e_n))$ d'où :

$$\text{covol}(\Lambda') = 2^n \text{covol}(\Lambda).$$

Ainsi $\text{covol}(\Lambda') < \mu(C)$, le théorème de Blichfeldt (sa contraposée) assure alors qu'il existe $(x, y) \in C^2$ tels que $x \neq y$ et $x - y \in 2\Lambda$.
Et donc par convexité symétrique de C :

$$\frac{x-y}{2} \in \Lambda \cap C \setminus \{0\}.$$

Si maintenant on suppose C compacte et l'inégalité large, on pose pour tout $p \in \mathbb{N}^*$:

$$C_p = \bigcup_{x \in C} B(x, \frac{1}{p}) = \{v \in \mathbb{R}^n \mid dist(v, C) < \frac{1}{p}\}$$

où $B(x, \frac{1}{p})$ est la boule euclidienne ouverte et la deuxième égalité définissant C_p repose sur le fait que la distance de v à C est atteinte par compacité de C.
Ainsi C_p est un ouvert mesurable borné (car C est bornée) et si on note $A_p = \{v \in \mathbb{R}^n \mid 0 < dist(v, C) < \frac{1}{p}\}$ on a (par fermeture de C) :

$$C_p = A_p \sqcup C$$

et A_p est un ouvert non vide (connexité de $\mathbb{R}^n$) donc $\mu(A_p) > 0$ et donc :

$$\mu(C_p) > \mu(C).$$

De plus la symétrie et la convexité de C entraîne celle de C_p (si $(x, y) \in C_p^2$ et $t \in [0, 1]$, soit $c_x, c_y \in C^2$ tels que $x \in B(c_x, \frac{1}{p})$ et $y \in B(c_y, \frac{1}{p})$ alors $tx + (1-t)y \in B(tc_x + (1-t)c_y, \frac{1}{p})$).
Ainsi par le théorème de Minkowski il existe x_p pour tout $p \in \mathbb{N}^*$ non nul dans $\Lambda \cap C_p$.
Or C_1 est borné donc $\Lambda \cap C_1$ est fini et comme pour tout $p \in \mathbb{N}^*$ on a $C_{p+1} \subset C_p$ alors l'ensemble $X = \{x_p \mid p \in \mathbb{N}^*\}$ est fini. On note $\{x_{p_1}, ..., x_{p_N}\}$ ses éléments.
Par l'absurde supposons que $X \cap C = \emptyset$ on aurait alors pour tout i que (toujours par fermeture de C) :

$$dist(x_{p_i}, C) > 0.$$

Mais donc en considérant alors $m = min_{i \in [[1,N]]}(dist(x_{p_i}, C))$ on a $m > 0$ donc il existe $P \in \mathbb{N}^*$ tel que $\frac{1}{P} < m$ mais alors on a $x_P \in X$ et donc $m \leq dist(x_P, C) < \frac{1}{P} < m$. C'est une contradiction.
Donc $X \cap C \neq \emptyset$. □

Proposition 1.2.9. *Soit Λ un réseau de $\mathbb{R}^n$ et $\Lambda' \subset \Lambda$ un sous-groupe alors les conditions suivantes sont équivalentes :*
i) Λ' est un réseau
ii) Λ' est d'indice fini dans Λ.
De plus si elles sont satisfaites alors : $[\Lambda : \Lambda'] = \frac{covol(\Lambda')}{covol(\Lambda)}$.

Démonstration. :
Dans un premier temps l'inclusion $\Lambda' \subset \Lambda$ implique que Λ' est discret.
ii) $\implies$ i) : On note $k = [\Lambda : \Lambda']$ on a alors par le théorème de Lagrange que $k\Lambda \subset \Lambda'$ et donc :

$$Vect(k\Lambda) = Vect(\Lambda) = \mathbb{R}^n \subset Vect(\Lambda').$$

Donc $Vect(\Lambda') = \mathbb{R}^n$ et Λ' est un réseau de $\mathbb{R}^n$.

$\boxed{\text{i)} \implies \text{ii)}}$: Découle du lemme 1.2.2 et du théorème 1.2.1.

Montrons maintenant que $k = [\Lambda : \Lambda'] = \frac{\text{covol}(\Lambda')}{\text{covol}(\Lambda)}$ on choisit $\lambda_1, ..., \lambda_k \in \Lambda$ des représentants de chaque classe d'équivalence de sorte que :

$$\Lambda = \coprod_{i=1}^{k} (\Lambda' + \lambda_i).$$

Soit X un domaine fondamental de Λ, on pose :

$$X' = \coprod_{i=1}^{k} (X + \lambda_i)$$

alors X' est mesurable et :

$$\mu(X') = k\mu(X).$$

On conclut car X' est un domaine fondamental de Λ' ; en effet :

$$\mathbb{R}^n = \coprod_{\lambda \in \Lambda} (X + \lambda) = \coprod_{i=1}^{k} \coprod_{\lambda' \in \Lambda'} (X + \lambda_i + \lambda') = \coprod_{\lambda' \in \Lambda'} (X' + \lambda').$$

□

1.3 Entiers sur un anneau commutatif

1.3.1 Fermeture intégrale

Définition 1.3.1 (Élément entier)**.** *Soit $\mathcal{R}$ un anneau et $\mathcal{A}$ un sous-anneau de $\mathcal{R}$, soit $x \in \mathcal{R}$ on dit que x est entier sur $\mathcal{A}$ s'il existe $P \in \mathcal{A}[X]$ unitaire tel que $P(x) = 0$.*

Remarque 1.3.1. Avec les notations précédentes la relation "$P(x) = 0$" est appelée une équation de dépendance intégrale de x sur $\mathcal{A}$.

Exemple 1.3.1. *On a que $x = \sqrt{2}$ est entier sur $\mathbb{Z}$ car $x^2 - 2 = 0$.*

Définition 1.3.2 (Anneau entier)**.** *Avec les notations précédentes on dit que $\mathcal{R}$ est entier sur $\mathcal{A}$ si tous les éléments de $\mathcal{R}$ sont entiers sur $\mathcal{A}$.*

Théorème 1.3.1 (Caractérisation des entiers)**.** *Soit $\mathcal{R}$ un anneau, et $\mathcal{A}$ un sous-anneau de $\mathcal{R}$ et $x \in \mathcal{R}$ alors les assertions suivantes sont équivalentes :*
i) L'élément x est entier sur $\mathcal{A}$.
ii) L'anneau $\mathcal{A}[x] = \{P(x) \mid P \in \mathcal{A}[X]\}$ est un $\mathcal{A}$-module de type fini.
iii) Il existe $\mathcal{C} \subset \mathcal{R}$ un sous-anneau de $\mathcal{R}$ contenant $\mathcal{A}$ et x qui est un $\mathcal{A}$-module de type fini.

Démonstration. :
i) $\implies$ ii) : On traduit l'équation de dépendance intégrale supposée de x sur $\mathcal{A}$:

$$\exists (a_{n-1}, ..., a_0) \in \mathcal{A}^n,\ x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 = 0\ (\heartsuit)$$

soit alors $\mathcal{M} =< 1, x, ..., x^{n-1} >$, le sous-module de $\mathcal{R}$ (on voit $\mathcal{R}$ comme un $\mathcal{A}$-module) engendré par $\{1, x, ..., x^{n-1}\}$. Montrons par récurrence forte sur j que pour tout $j \geq 0,\ x^{n+j} \in \mathcal{M}$.
Initialisation : par $(\heartsuit)$ on a :

$$x^n = -\sum_{i=0}^{n-1} a_i x^i \in \mathcal{M}.$$

Hérédité : Soit $j \geq 1$ tel que pour tout $k \in [[0, j[[,\ x^{n+k} \in \mathcal{M}$ alors en multipliant $(\heartsuit)$ par x^j on obtient :

$$x^{n+j} = -\sum_{i=0}^{n-1} a_i x^{i+j}.$$

Or pour tout $i \in [[0, n-1]], i + j < n + j$ donc $x^{i+j} \in \mathcal{M}$ et donc $-\sum_{i=0}^{n-1} a_i x^{i+j} \in \mathcal{M}$ et finalement on a bien que : $\forall j \in \mathbb{N},\ x^{n+j} \in \mathcal{M}$. On a donc montré que $\mathcal{X} = \{x^k \mid k \in \mathbb{N}\} \subset \mathcal{M}$ donc :

$$\mathcal{A}[x] =< \mathcal{X} > \subset \mathcal{M}$$

mais on a aussi :

$$\mathcal{M} =< \{1, x, ..., x^{n-1}\} > \subset < \mathcal{X} >= \mathcal{A}[x]$$

donc finalement $\mathcal{A}[x] = \mathcal{M}$ et est de type fini.
ii) $\implies$ iii) : On voit que prendre $\mathcal{C} = \mathcal{A}[x]$ convient.
iii) $\implies$ i) : Soit $(y_1, ..., y_n) \in \mathcal{C}^n$ tels que :

$$\mathcal{C} = \sum_{i=1}^{n} \mathcal{A} y_i$$

comme $x \in \mathcal{C}$ et pour tout $i \in [[1, n]], y_i \in \mathcal{C}$ on a que pour tout $i \in [[1, n]], xy_i \in \mathcal{C}$ de sorte qu'il existe $(a_{i,j})_{1 \leq j \leq n} \in \mathcal{A}^n$ tels que :

$$xy_i = \sum_{j=1}^{n} a_{i,j} y_j.$$

On traduit cela en écrivant :

$$\forall i \in [[1,n]],\ \sum_{j=1}^{n}(\delta_{ij}x - a_{i,j})y_j = 0.\ (\clubsuit)$$

(Avec δ_{ij} le symbole de Kronecker.)
Soit alors $M = (\delta_{ij}x - a_{i,j})_{1\leq i,j\leq n} \in \mathcal{M}_n(\mathcal{C})$ et $d = \det(M)$ son déterminant
on peut retraduire ($\clubsuit$) par :

$$M\begin{pmatrix} y_1 \\ ... \\ y_n \end{pmatrix} = \begin{pmatrix} 0 \\ ... \\ 0 \end{pmatrix}$$

(système de n équations linéaire homogènes en $(y_1, ..., y_n)$).
Alors en multipliant par $\mathrm{com}(M)^T$ et en utilisant la formule de la comatrice on obtient :

$$\mathrm{com}(M)^T M\begin{pmatrix} y_1 \\ ... \\ y_n \end{pmatrix} = dI_n\begin{pmatrix} y_1 \\ ... \\ y_n \end{pmatrix} = \begin{pmatrix} dy_1 \\ ... \\ dy_n \end{pmatrix} = \begin{pmatrix} 0 \\ ... \\ 0 \end{pmatrix}$$

donc on en déduit :

$$\forall i \in [[1,n]],\ dy_i = 0.$$

Mais alors comme $\mathcal{C} = \sum_{i=1}^{n} \mathcal{A}y_i$ on a que pour tout $c \in \mathcal{C}$, $dc = 0$ et en particulier $d1_{\mathcal{R}} = d = 0$.
Or si on développe $d = \det(M)$ on a :

$$d = 0 = \sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma)\prod_{i=1}^{n}(\delta_{\sigma(i)i}x - a_{\sigma(i),i})$$

on obtient bien une équation de dépendance intégrale de la forme "$P(x) = 0$" où $P \in \mathcal{A}[X]$ est unitaire de degré n car on obtient le coefficient devant X^n avec $\sigma = Id_n$:

$$P = \prod_{i=1}^{n}(X - a_{i,i}) + \sum_{\substack{\sigma\in\mathfrak{S}_n \\ \sigma\neq Id_n}} \varepsilon(\sigma)\prod_{i=1}^{n}(\delta_{\sigma(i)i}X - a_{\sigma(i),i}).$$

□

Définition 1.3.3 (Fermeture intégrale)**.** *Soit $\mathcal{R}$ un anneau, et $\mathcal{A}$ un sous-anneau de $\mathcal{R}$, on définit $\mathcal{A}'$ la fermeture intégrale de $\mathcal{A}$ dans $\mathcal{R}$ comme étant l'ensemble des entiers sur $\mathcal{A}$:*

$$\mathcal{A}' = \{x \in \mathcal{R} \mid x \text{ entier sur } \mathcal{A}\}.$$

Remarque 1.3.2. En considérant les polynômes $X - a$ avec $a \in \mathcal{A}$ on a que $\mathcal{A} \subset \mathcal{A}'$.

Remarque 1.3.3. Avec les notations précédentes si $\mathcal{C}$ est un sous-anneau de $\mathcal{R}$, entier sur $\mathcal{A}$ on remarque alors que $\mathcal{C} \subset \mathcal{A}'$.

Théorème 1.3.2. *Soit $\mathcal{R}$ un anneau, $\mathcal{A}$ un sous-anneau de $\mathcal{R}$ et $(x_i)_{1\leq i\leq n}$ une famille finie d'éléments de $\mathcal{R}$. Si x_1 est entier sur $\mathcal{A}$ et pour tout $i \in [[2,n]]$, x_i est entier sur $\mathcal{A}[x_1, ..., x_{i-1}]$ (en particulier si tous les x_i sont entiers sur A), alors :*

$$\mathcal{A}[x_1, ..., x_n]$$

est un $\mathcal{A}$-module de type fini.

Démonstration. :
On raisonne par récurrence sur n.
Initialisation : pour $n = 1$ c'est l'implication i) $\implies$ ii) du théorème 1.3.1.
Hérédité : soit $n \geq 2$, supposons le théorème 1.3.2 vrai pour toute famille de $n-1$ éléments, soit alors $(x_i)_{1\leq i\leq n}$ une famille de n éléments de $\mathcal{R}$ qui vérifie les hypothèses du théorème 1.3.2.

Alors, $\mathcal{C} = \mathcal{A}[x_1, ..., x_{n-1}]$ est un $\mathcal{A}$-module de type fini par hypothèse de récurrence sur $(x_i)_{1\leq i\leq n-1}$.
Soit alors $(c_1, ..., c_p) \in \mathcal{C}^p$ tels que :

$$\mathcal{C} = \sum_{j=1}^{p} \mathcal{A}c_j.$$

Ensuite par application du cas $n = 1$ avec x_n et $\mathcal{C}$ on a que :

$$\mathcal{A}[x_1, ..., x_n] = \mathcal{C}[x_n]$$

est un $\mathcal{C}$-module de type fini, soit alors $(y_1, ..., y_k) \in \mathcal{C}[x_n]^k$ tels que $\mathcal{C}[x_n] = \sum_{i=1}^{k} \mathcal{C}y_i$.
Donc :

$$\mathcal{A}[x_1, ..., x_n] = \mathcal{C}[x_n] = \sum_{i=1}^{k} \mathcal{C}y_i = \sum_{i=1}^{k}(\sum_{j=1}^{p} \mathcal{A}c_j)y_i = \sum_{(i,j)\in[[1,k]]\times[[1,p]]} \mathcal{A}(c_j y_i).$$

Ainsi $(c_j y_i)_{(i,j)\in[[1,k]]\times[[1,p]]}$ engendre le $\mathcal{A}$-module $\mathcal{A}[x_1, ..., x_n]$. □

Corollaire 1.3.1. *Soit $\mathcal{R}$ un anneau, $\mathcal{A}$ un sous-anneau de $\mathcal{R}$, soit également $(x, y) \in \mathcal{R}^2$ deux éléments de $\mathcal{R}$ entiers sur $\mathcal{A}$. Alors $x + y,\ x - y$ et xy sont entiers sur $\mathcal{A}$.*

Démonstration. :
En effet, $x + y,\ x - y$ et xy appartiennent à $\mathcal{A}[x, y]$ qui est un $\mathcal{A}$-module de type fini par le théorème 1.3.2 et donc par l'implication $\boxed{\text{iii)} \implies \text{i)}}$ du théorème 1.3.1 on a que $x + y,\ x - y$ et xy sont entiers sur $\mathcal{A}$. □

Corollaire 1.3.2. *Soit $\mathcal{R}$ un anneau, $\mathcal{A}$ un sous-anneau de $\mathcal{R}$ alors $\mathcal{A}'$ la fermeture intégrale de $\mathcal{A}$ dans $\mathcal{R}$ est un sous-anneau de $\mathcal{R}$ (contenant $\mathcal{A}$).*

Théorème 1.3.3 (Transitivité)**.** *Soit $\mathcal{R}$ un anneau, $\mathcal{C}$ un sous-anneau de $\mathcal{R}$ et $\mathcal{A}$ un sous-anneau de $\mathcal{C}$ alors :*

$$(\mathcal{R} \text{ est entier sur } \mathcal{C} \text{ et } \mathcal{C} \text{ est entier sur } \mathcal{A}) \implies \mathcal{R} \text{ est entier sur } \mathcal{A}.$$

Démonstration. :
Soit $x \in \mathcal{R}$, il est entier sur $\mathcal{C}$ on a donc une équation de dépendance intégrale de la forme :

$$x^n + c_{n-1}x^{n-1} + ... + c_1 x + c_0 = 0,\ (c_{n-1}, ..., c_0) \in \mathcal{C}^n.$$

Posons $\mathcal{D} = \mathcal{A}[c_{n-1}, ..., c_0]$ alors x est aussi entier sur $\mathcal{D}$.
Comme $\mathcal{C}$ est entier sur $\mathcal{A}$, les $(c_i)_{0\leq i\leq n-1}$ sont entiers sur $\mathcal{A}$ donc par le théorème 1.3.2 :

$$\mathcal{D}[x] = \mathcal{A}[c_0, ..., c_{n-1}, x]$$

est un $\mathcal{A}$-module de type fini et donc par l'implication iii) $\implies$ i) du théorème 1.3.1, x est entier sur $\mathcal{A}$. □

1.3.2 Anneaux intégralement clos

Définition 1.3.4 (Clôture intégrale)**.** *Soit $\mathcal{A}$ un anneau intègre et $\mathcal{R} = \mathcal{K}_\mathcal{A}$ le corps des fractions de $\mathcal{A}$, on parle de clôture intégrale pour désigner la fermeture intégrale $\mathcal{A}'$ de $\mathcal{A}$ dans $\mathcal{R}$.*

Définition 1.3.5 (Anneau intégralement clos)**.** *On dit que $\mathcal{A}$ (intègre) est intégralement clos ou normal s'il est égal à sa clôture intégrale.*

Exemple 1.3.2. *L'anneau $\mathcal{A} = \mathbb{Z}[i\sqrt{3}]$ n'est pas intégralement clos, car $j = \frac{-1+i\sqrt{3}}{2} \in \mathbb{Q}(i\sqrt{3})$ et vérifie $j^2 + j + 1 = 0$.*

Exemple 1.3.3. *Avec les notations précédentes, la clôture intégrale $\mathcal{A}'$ de $\mathcal{A}$ est intégralement close. En effet, on remarque d'abord que $\mathcal{K}_{\mathcal{A}'} = \mathcal{K}_{\mathcal{A}}$ puis que la clôture intégrale de $\mathcal{A}'$: $(\mathcal{A}')'$ est entière sur $\mathcal{A}'$ donc par transitivité sur $\mathcal{A}$ et donc $(\mathcal{A}')' = \mathcal{A}'$.*

Proposition 1.3.1. *Soit $\mathcal{A}$ un anneau, on a l'implication suivante :*

$$\mathcal{A} \text{ factoriel} \implies \mathcal{A} \text{ intégralement clos.}$$

Démonstration. :
Soit $x \in \mathcal{K}_{\mathcal{A}}$ entier sur $\mathcal{A}$.
Comme $\mathcal{A}$ est factoriel, il existe $(p, q) \in \mathcal{A}^2$ premiers entre eux tels que $x = \frac{p}{q}$.
On traduit l'équation de dépendance intégrale supposée de x sur $\mathcal{A}$:

$$\exists (a_{n-1}, ..., a_0) \in \mathcal{A}^n,\ (\frac{p}{q})^n + a_{n-1}(\frac{p}{q})^{n-1} + ... + a_1\frac{p}{q} + a_0 = 0\ (\heartsuit)$$

on en déduit, en multipliant $(\heartsuit)$ par q^n :

$$p^n = -a_{n-1}p^{n-1}q - ... - a_1pq^{n-1} - a_0q^n$$

donc $q \mid p^n$, comme p et q sont premiers entre eux, le lemme de Gauβ implique alors que $q \mid p$ et donc q est inversible, soit alors $u \in \mathcal{A}$ tel que $qu = 1$ on a alors $x = \frac{p}{q} = \frac{pu}{qu} = pu \in \mathcal{A}$. □

Proposition 1.3.2. *Soit $\mathcal{R}$ un anneau intègre et $\mathcal{A}$ un sous-anneau de $\mathcal{R}$, tel que $\mathcal{R}$ soit entier sur $\mathcal{A}$. Alors :*

$\mathcal{R}$ est un corps, si et seulement si, $\mathcal{A}$ est un corps.

Démonstration. :
$\Longleftarrow$: Soit $x \in \mathcal{R}$, $x \neq 0$ comme x est entier sur $\mathcal{A}$ on a par le théorème 7 que $\mathcal{A}[x]$ est un $\mathcal{A}$-module de type fini donc comme $\mathcal{A}$ est un corps, $\mathcal{A}[x]$ est un $\mathcal{A}$-espace vectoriel de dimension finie.
D'autre part, $y \mapsto xy$ est une application $\mathcal{A}$-linéaire de $\mathcal{A}[x]$ dans lui-même, qui est injective car $\mathcal{A}[x]$ est intègre et car $x \neq 0$. Elle est donc surjective, et donc 1 admet un antécédent et donc x est inversible dans $\mathcal{R}$.
$\Longrightarrow$: Soit $a \in \mathcal{A}$, $a \neq 0$ et $x = a^{-1} \in \mathcal{R}$ l'inverse de a dans $\mathcal{R}$, qui satisfait une équation de dépendance intégrale supposée :

$$\exists (a_{n-1}, ..., a_0) \in \mathcal{A}^n,\ x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0 = 0\ (\heartsuit)$$

en multipliant $(\heartsuit)$ par a^{n-1}, on obtient :

$$x = -a_{n-1} - ... - a_1a^{n-2} - a_0a^{n-1} \in \mathcal{A}.$$

□

1.3.3 Anneaux de Dedekind

Définition 1.3.6 (Idéal de type fini)**.** *Soit $\mathcal{A}$ un anneau et $\mathcal{I}$ un idéal de $\mathcal{A}$ on dit qu'il est de type fini si il est de type fini vu comme un sous-module du $\mathcal{A}$-module $\mathcal{A}$.*

Définition 1.3.7 (Anneau noethérien)**.** *Soit $\mathcal{A}$ un anneau, on dit que $\mathcal{A}$ est noethérien si il vérifie l'une des trois conditions suivantes équivalentes :*
1) Tout idéal de $\mathcal{A}$ est de type fini.
2) Toute suite croissante $\mathcal{I}_1 \subset \mathcal{I}_2 \subset ... \subset \mathcal{I}_n \subset ...$ d'idéaux de $\mathcal{A}$ est stationnaire.
3) Tout ensemble non vide d'idéaux de $\mathcal{A}$ a un élément maximal pour l'inclusion.

Remarque 1.3.4. [Preuve que les définitions sont équivalentes]
$\boxed{1) \implies 2)}$: Soit $(\mathcal{I}_n)_{n\in\mathbb{N}}$ une suite croissante d'idéaux de $\mathcal{A}$ la suite étant croissante l'ensemble $\mathcal{I} = \bigcup_{n\in\mathbb{N}} \mathcal{I}_n$ est un idéal de $\mathcal{A}$ il est donc de type fini, soit alors $(a_1, ..., a_k) \in \mathcal{A}^k$ tels que :

$$\mathcal{I} = (a_1, .., a_k).$$

Alors, toujours par croissance de la suite, il existe $N \in \mathbb{N}$ tel que $a_1, ..., a_k \in \mathcal{I}_N$ mais alors $\mathcal{I} = \mathcal{I}_N$.
$\boxed{2) \implies 3)}$: Soit E un ensemble non vide d'idéaux. Supposons que E n'ait pas d'élément maximal.
On construit alors par récurrence une suite $(\mathcal{I}_n)_{n\in\mathbb{N}}$ qui contredit 2) : on prend $\mathcal{I}_1 \in E$ quelconque, puis, comme $\mathcal{I}_1$ n'est pas maximal on trouve $\mathcal{I}_2 \in E$ tel que $\mathcal{I}_1 \subsetneq \mathcal{I}_2$ puis, comme $\mathcal{I}_2$ n'est pas maximal on trouve $\mathcal{I}_3 \in E$ tel que $\mathcal{I}_2 \subsetneq \mathcal{I}_3$, et ainsi de suite ...
$\boxed{3) \implies 1)}$: Soit $\mathcal{I}$ un idéal de $\mathcal{A}$ et :

$$E = \{\mathcal{J} \mid \mathcal{J} \text{ idéal de } \mathcal{A},\ \mathcal{J} \subset \mathcal{I},\ \mathcal{J} \text{ est de type fini}\}.$$

Alors $E \neq \emptyset$ car $(0) \in E$. Soit $\mathcal{J}$ un élément maximal de E, supposons que $\mathcal{J} \subsetneq \mathcal{I}$ soit alors $a \in \mathcal{I}\backslash\mathcal{J}$ alors $\mathcal{J} + (a)$ est un idéal qui est encore de type fini, encore inclus dans $\mathcal{I}$ mais $\mathcal{J} \subsetneq \mathcal{J} + (a)$ contredisant alors le fait que $\mathcal{J}$ est un élément maximal donc $\mathcal{I} = \mathcal{J}$ et $\mathcal{I}$ est de type fini.

Exemple 1.3.4. *Tout anneau principal est noethérien.*

Proposition 1.3.3. *Soit $\mathcal{A}$ un anneau noethérien et $\mathcal{I}$ un idéal de $\mathcal{A}$ alors $\mathcal{A}/\mathcal{I}$ est noethérien.*

Démonstration. :
On note $\pi : \mathcal{A} \to \mathcal{A}/\mathcal{I}$, $a \mapsto \overline{a}$ la projection canonique.
Soit $\mathcal{J} \subset \mathcal{A}/\mathcal{I}$ un idéal de $\mathcal{A}/\mathcal{I}$ alors $\pi^{-1}(\mathcal{J})$ est un idéal de $\mathcal{A}$ par conséquent il est de type fini, soit donc $(a_1, ..., a_k) \in \mathcal{A}^k$ tels que :

$$\pi^{-1}(\mathcal{J}) = (a_1, ..., a_k).$$

Alors on a :

$$\mathcal{J} = (\overline{a_1}, ..., \overline{a_k}).$$

□

Pour la suite on introduit la notation suivante : si $P \in \mathcal{A}[X]$ est un polynôme non nul à coefficients dans $\mathcal{A}$ on note $\mathrm{dom}(P)$ le coefficient dominant de P.

Lemme 1.3.1. *Soit $\mathcal{A}$ un anneau et $\mathcal{I}$ et $\mathcal{J}$ deux idéaux de $\mathcal{A}[X]$. On définit pour tout $n \in \mathbb{N}$:*

$$d_n(\mathcal{I}) = \{a \in \mathcal{A}\backslash\{0\} \mid \exists (a_0, ..., a_{n-1}) \in \mathcal{A}^n,\ aX^n + \sum_{i=0}^{n-1} a_i X^i \in \mathcal{I}\} \cup \{0\}.$$

Plus simplement $d_n(\mathcal{I}) = \{dom(P) \mid P \in \mathcal{I},\ deg(P) = n\} \cup \{0\}$.
Alors on a :
0) Pour tout $n \in \mathbb{N}$, $d_n(\mathcal{I})$ est un idéal de $\mathcal{A}$
1) $\mathcal{I} \subset \mathcal{J} \implies \forall n \in \mathbb{N},\ d_n(\mathcal{I}) \subset d_n(\mathcal{J})$
2) Pour tout $n \in \mathbb{N}$, $d_n(\mathcal{I}) \subset d_{n+1}(\mathcal{I})$
3) Si $\mathcal{I} \subset \mathcal{J}$ alors on a ($\mathcal{I} = \mathcal{J}$ si et seulement si $\forall n \in \mathbb{N},\ d_n(\mathcal{I}) = d_n(\mathcal{J})$)

Démonstration. :
$\boxed{0)}$: Soit $n \in \mathbb{N}$, alors par définition $0 \in d_n(\mathcal{I})$. Soit $(a, b) \in d_n(\mathcal{I})^2$, si a ou b est nul alors il est clair que $a - b \in d_n(\mathcal{I})$, on suppose donc a et b non nuls, soit alors $(P, Q) \in \mathcal{I}^2$ tels que $a = \mathrm{dom}(P)$ et $b = \mathrm{dom}(Q)$ et $\deg(P) = \deg(Q) = n$. Si $a - b = 0$, alors $a - b \in d_n(\mathcal{I})$ sinon, $\mathrm{dom}(P - Q) = a - b$ et $\deg(P - Q) = n$ (car on suppose $a - b \neq 0$) et $P - Q \in \mathcal{I}$ donc dans tous les cas $a - b \in d_n(\mathcal{I})$.
Ainsi, $d_n(\mathcal{I})$ est un sous-groupe de $\mathcal{A}$ montrons qu'il est stable par multiplication externe. Soit $a \in d_n(\mathcal{I})$ et $x \in \mathcal{A}$, si $ax = 0$ alors $ax \in d_n(\mathcal{I})$, on suppose donc $ax \neq 0$ (donc en particulier $x \neq 0$ et $a \neq 0$) soit alors $P \in \mathcal{I}$ tel que $a = \mathrm{dom}(P)$ et $\deg(P) = n$, alors $ax = \mathrm{dom}(xP)$ or $\deg(xP) = n$ (car $ax \neq 0$) et $xP \in \mathcal{I}$ car $\mathcal{I}$ est un idéal et donc $ax \in d_n(\mathcal{I})$ dans tous les cas.
$\boxed{1)}$: Immédiat
$\boxed{2)}$: Soit $n \in \mathbb{N}$ et $a \in d_n(\mathcal{I})$ si $a = 0$ alors (toujours par définition) $a \in d_{n+1}(\mathcal{I})$ et si $a \neq 0$, soit $P \in \mathcal{I}$ tel que $a = \mathrm{dom}(P)$ et $\deg(P) = n$ alors on a aussi $a = \mathrm{dom}(XP)$ et $\deg(XP) = \deg(X) + \deg(P) = 1 + n$ et $XP \in \mathcal{I}$ et donc $a \in d_{n+1}(\mathcal{I})$.
$\boxed{3)}$: On suppose $\mathcal{I} \subset \mathcal{J}$. Montrons l'équivalence souhaitée :

$\boxed{\Longrightarrow}$: Immédiat
$\boxed{\Longleftarrow}$: On note $\mathcal{P}(n)$ le prédicat suivant :

$$\mathcal{P}(n) : (\forall P \in \mathcal{J},\ \deg(P) = n \implies P \in \mathcal{I}).$$

Le fait que $d_0(\mathcal{I}) = d_0(\mathcal{J})$ implique $\mathcal{P}(0)$. Soit $n \in \mathbb{N}$ tel que $\mathcal{P}(k)$ soit vrai pour tout $k \leq n$ montrons $\mathcal{P}(n+1)$: soit $P \in \mathcal{J}$ tel que $\deg(P) = n+1$, comme on a $d_{n+1}(\mathcal{I}) = d_{n+1}(\mathcal{J})$ il existe $Q \in \mathcal{I}$ tel que $\mathrm{dom}(P) = \mathrm{dom}(Q)$ et $\deg(Q) = n+1$ mais alors $k = \deg(P-Q) \leq n$ et $P - Q \in \mathcal{J}$ donc par $\mathcal{P}(k)$ on a $P - Q \in \mathcal{I}$ mais alors $P = (P-Q) + Q \in \mathcal{I}$. Ce qui montre $\mathcal{P}(n)$ par récurrence que pour tout $n \in \mathbb{N}$ et ainsi $\mathcal{I} = \mathcal{J}$.

□

Théorème 1.3.4 (Théorème de la base de Hilbert)**.** *Soit $\mathcal{A}$ un anneau, on a l'implication suivante :*

$$\mathcal{A} \text{ noethérien} \implies \mathcal{A}[X] \text{ noethérien.}$$

Démonstration. :
Soit $(\mathcal{I}_n)_{n\in\mathbb{N}}$ une suite croissante d'idéaux de $\mathcal{A}[X]$.
$\mathcal{A}$ étant noethérien la famille $(d_k(\mathcal{I}_n))_{(k,n)\in\mathbb{N}\times\mathbb{N}}$ admet un élément maximal $d_l(\mathcal{I}_m)$ $((l,m) \in \mathbb{N}^2)$.
De plus, pour $k \leq l$, la suite $(d_k(\mathcal{I}_n))_{n\in\mathbb{N}}$ est croissante donc stationnaire, donc il existe n_k tel que pour tout $n \geq n_k$, $d_k(\mathcal{I}_n) = d_k(\mathcal{I}_{n_k})$.
On pose alors :

$$N = max(m, n_0, ..., n_l).$$

Montrons alors que pour tout $n \geq N$, $\mathcal{I}_n = \mathcal{I}_N$:
Comme $\mathcal{I}_N \subset \mathcal{I}_n$, il suffit par le lemme précédent de montrer que :

$$\forall k \in \mathbb{N},\ d_k(\mathcal{I}_n) = d_k(\mathcal{I}_N).$$

Si $k \geq l$: on a :

$$d_l(\mathcal{I}_m) \subset d_k(\mathcal{I}_m) \subset d_k(\mathcal{I}_N) \subset d_k(\mathcal{I}_n)$$

et comme $d_l(\mathcal{I}_m)$ est maximal :

$$d_k(\mathcal{I}_n) = d_l(\mathcal{I}_m) = d_k(\mathcal{I}_N).$$

Si $k < l$: on a :

$$d_k(\mathcal{I}_N) = d_k(\mathcal{I}_{n_k}) = d_k(\mathcal{I}_n)$$

□

Définition 1.3.8 (Anneau de Dedekind)**.** *Soit $\mathcal{A}$ un anneau intègre, on dit que c'est un anneau de Dedekind s'il vérifie les trois propriétés suivantes :*
1) $\mathcal{A}$ est noethérien.
2) $\mathcal{A}$ est intégralement clos.
3) Tout idéal premier non nul de $\mathcal{A}$ est maximal.

Définition 1.3.9 (Anneau de dimension 1)**.** *Un anneau $\mathcal{A}$ qui vérifie que tout idéal premier non nul est maximal est dit de dimension* 1.

Exemple 1.3.5. *L'anneau $\mathbb{Z}$ est de dimension* 1.

Exemple 1.3.6. *Plus généralement tout anneau principal est de Dedekind.*

Proposition 1.3.4. *Soit $\mathcal{R}$ un anneau intègre et $\mathcal{A}$ un sous-anneau de $\mathcal{R}$, tel que $\mathcal{R}$ soit entier sur $\mathcal{A}$. Alors :*

$$\mathcal{A} \text{ est de dimension } 1 \implies \mathcal{R} \text{ est de dimension } 1.$$

Démonstration. :
Soit $\mathcal{I} \subset \mathcal{R}$ un idéal premier non nul de $\mathcal{R}$, soit alors $x \in \mathcal{I}, x \neq 0$ on traduit l'équation de dépendance intégrale supposée de x sur $\mathcal{A}$:

$$\exists n \geq 1,\ \exists (a_{n-1}, ..., a_0) \in \mathcal{A}^n,\ x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 = 0\ (\heartsuit)$$

quitte à simplifier par une puissance de x on peut supposer $a_0 \neq 0$ et alors ($\heartsuit$) se réécrit :

$$a_0 = -x(a_1 + xa_2 + ... + x^{n-1}) \in \mathcal{I} \cap \mathcal{A}.$$

Or on vérifie aisément que $\mathcal{I} \cap \mathcal{A}$ est un idéal premier (non nul car contenant a_0) de $\mathcal{A}$ donc $\mathcal{I} \cap \mathcal{A}$ est un idéal maximal de $\mathcal{A}$ or :

$$\varphi : \mathcal{A}/(\mathcal{I} \cap \mathcal{A}) \to \mathcal{R}/\mathcal{I}$$
$$x + \mathcal{I} \cap \mathcal{A} \mapsto x + \mathcal{I}$$

est une injection, donc par abus de notation : $\mathcal{A}/(\mathcal{I} \cap \mathcal{A}) \subset \mathcal{R}/\mathcal{I}$ mais alors $\mathcal{R}/\mathcal{I}$ est entier sur $\mathcal{A}/(\mathcal{I} \cap \mathcal{A})$ par réduction modulo $\mathcal{I}$ des équations de dépendances intégrales. Mais alors comme $\mathcal{A}/(\mathcal{I} \cap \mathcal{A})$ est un corps on a en vertu de la proposition 1.3.2 que $\mathcal{R}/\mathcal{I}$ est un corps et donc $\mathcal{I}$ est maximal. □

Proposition 1.3.5. *Soit $\mathcal{A}$ un anneau de Dedekind, on a l'équivalence suivante :*

$\mathcal{A}$ est principal, si et seulement si, $\mathcal{A}$ est factoriel.

Démonstration. :
$\boxed{\Longrightarrow}$: C'est un fait général connu qui ne nécessite pas d'être de Dedekind.
$\boxed{\Longleftarrow}$: Montrons dans un premier temps que les idéaux maximaux de $\mathcal{A}$ sont principaux.
Soit $\mathcal{I} \subset \mathcal{A}$ un idéal maximal non nul (s'il est nul il n'y a rien à montrer) et $x \in \mathcal{I}$, $x \neq 0$. Comme $\mathcal{A}$ est factoriel on peut écrire $x = up_1...p_r$ avec $u \in \mathcal{A}^\times$ et les p_i irréductibles. Comme $\mathcal{I}$ est premier (car maximal) l'un des $p_i \in \mathcal{I}$ (on ne peut avoir pas $u \in \mathcal{I}$ sinon on aurait $\mathcal{I} = \mathcal{A}$), supposons donc (quitte à renuméroter) que $p_1 \in \mathcal{I}$ on a alors :

$$(0) \subset (p_1) \subset \mathcal{I}$$

avec (p_1) premier non nul (car $\mathcal{A}$ est factoriel) donc maximal car $\mathcal{A}$ est de Dedekind (donc de dimension 1) et donc :

$$\mathcal{I} = (p_1).$$

On note pour $n \geq 1$, $\mathcal{P}(n)$ le prédicat suivant : tout idéal de $\mathcal{A}$ engendré par n éléments est principal.
Montrons $\mathcal{P}(2)$:
Soit $\mathcal{J} = (x, y)$ avec $(x, y) \in \mathcal{A}^2$, soit $d = pgcd(x, y)$ (qui existe car $\mathcal{A}$ est factoriel) et $(x', y') \in \mathcal{A}^2$ tels que $x = dx'$ et $y = dy'$ avec $pgcd(x', y') = 1$. On a donc $\mathcal{J} \subset (d)$ et $(x', y') \subset (1)$; si on suppose $(x', y') \subsetneq (1)$ alors par le théorème de Krull il existe $\mathcal{M}$ maximal tel que $(x', y') \subset \mathcal{M}$, or par ce qui précède $\mathcal{M}$ est principal. Soit donc p irréductible tel que $\mathcal{M} = (p)$; alors $(x', y') \subset (p)$ donc $p \mid x'$ et $p \mid y'$ donc p est inversible (absurde car p est irréductible) donc :

$$(x', y') = (1).$$

On a donc une relation de Bézout :

$$1 = ux' + vy' \ (u, v) \in \mathcal{A}^2$$

d'où :

$$d = ux + vy \in \mathcal{J}$$

et donc :

$$(d) = \mathcal{I}.$$

Enfin, si $(a_1, ..., a_{n+1}) \in \mathcal{A}^{n+1}$ comme :

$$(a_1, ..., a_{n+1}) = (a_1, ..., a_n) + (a_{n+1})$$

il est clair que $\mathcal{P}(2) \implies (\forall n \geq 2,\ \mathcal{P}(n) \implies \mathcal{P}(n+1))$ et donc on conclut par récurrence qu'on a pour tout $n \geq 2$, $\mathcal{P}(n)$.
Soit maintenant $\mathcal{I} \subset \mathcal{A}$ un idéal quelconque. Comme $\mathcal{A}$ est noethérien, il existe $(a_1, ..., a_n) \in \mathcal{A}^n$ tels que

$$\mathcal{I} = (a_1, ..., a_n)$$

et donc par ce qui précède $\mathcal{I}$ est principal. □

On rappelle le résultat suivant sur les anneaux factoriels.

Proposition 1.3.6. *Soit $\mathcal{A}$ un anneau intègre, alors $\mathcal{A}$ est factoriel si et seulement si les deux conditions suivantes sont vérifiées :*

(1) tout élément non nul $a \in \mathcal{A}$ peut s'écrire

$$a = u\pi_1 ... \pi_r$$

où $\pi_1, ..., \pi_r$ sont irréductibles et $u \in \mathcal{A}^\times$
(2) tout élément irréductible est premier.

On rappelle également que :

Proposition 1.3.7. *Soit $\mathcal{A}$ un anneau intègre noethérien. Alors, tout élément $a \in \mathcal{A}$ non nul admet une factorisation de la forme*

$$a = u\pi_1 ... \pi_r$$

où $\pi_1, ..., \pi_r$ sont irréductibles et $u \in \mathcal{A}^\times$.

Pour une preuve on pourra consulter [1] ou [5].
En combinant les deux résultats précédents on obtient :

Corollaire 1.3.3. *Soit $\mathcal{A}$ un anneau de Dedekind. Si tout élément irréductible est premier, alors $\mathcal{A}$ est factoriel.*

Chapitre 2

Les corps quadratiques

2.1 Les anneaux d'entiers des corps quadratiques

2.1.1 Les corps quadratiques

Définition 2.1.1 (Corps de nombres)**.** *On appelle corps de nombres une extension finie $\mathcal{K}$ de $\mathbb{Q}$.*
(i.e un corps $\mathcal{K}$ qui contient $\mathbb{Q}$ et est un $\mathbb{Q}$-espace vectoriel de dimension finie.)

Définition 2.1.2 (Anneau des entiers)**.** *Soit $\mathcal{K}$ un corps de nombres, on appelle anneau des entiers du corps $\mathcal{K}$ la fermeture de $\mathbb{Z}$ dans $\mathcal{K}$.*
Donc si on note $\mathcal{A}$ l'anneau des entiers du corps $\mathcal{K}$ on a :

$$\mathcal{A} = \{x \in \mathcal{K} \mid x \text{ entier sur } \mathbb{Z}\}.$$

Remarque 2.1.1. Avec les notations précédentes $\mathcal{A}$ est intégralement clos.
(C'est le même raisonnement que l'exemple 1.3.3.)

Proposition 2.1.1. *Soit $\mathcal{K}$ un sous-corps de $\mathbb{C}$, et soit $d \in \mathcal{K}$.*
Deux racines carrées de d dans $\mathbb{C}$ différant seulement par un signe, elles engendrent la même sous-extension. Par commodité, on note $\sqrt{d} \in \mathbb{C}$ un nombre complexe de carré d.
Alors, on a l'égalité :

$$\mathcal{K}(\sqrt{d}) = \{a + b\sqrt{d} \mid (a,b) \in \mathcal{K}^2\}.$$

En particulier $[\mathcal{K}(\sqrt{d}) : \mathcal{K}] \leq 2$.

Démonstration. :
Si $\sqrt{d} \in \mathcal{K}$, alors $\mathcal{K}(\sqrt{d}) = \mathcal{K}$, et il n'y a rien à faire.
On suppose donc que $\sqrt{d} \notin \mathcal{K}$, l'inclusion "$\supset$" étant triviale, montrons l'autre inclusion.
Il suffit pour cela de démontrer que :

$$\{a + b\sqrt{d} \mid (a,b) \in \mathcal{K}^2\}$$

est un sous-corps de $\mathbb{C}$ contenant $\mathcal{K}$ et $\sqrt{d}$.
Tous les points à vérifier sont immédiats, sauf la stabilité par passage à l'inverse.
Supposons que $z = a + b\sqrt{d} \neq 0$, $((a,b) \in \mathcal{K}^2)$ alors $a^2 - db^2 \neq 0$.
En effet, si on avait $a^2 - db^2 = 0$, alors $b \neq 0$ (sinon $a = 0$ et $z = 0$), et par conséquent d serait le carré d'un élément de $\mathcal{K}$, ce qui entraînerait alors que $\sqrt{d} \in \mathcal{K}$.
Mais alors, on vérifie que l'on a

$$z^{-1} = \frac{a - b\sqrt{d}}{a^2 - db^2} \in \{a + b\sqrt{d} \mid (a,b) \in \mathcal{K}^2\}$$

□

Définition 2.1.3 (Corps quadratiques). *On désigne par corps quadratique les corps de nombres de la forme $\mathbb{Q}(\sqrt{d})$ où $d \in \mathbb{Z}\backslash\{0,1\}$ est sans facteur carré. (Par ce qui précède ce sont des sous-corps de $\mathbb{C}$ de $\mathbb{Q}$-dimension 2.)*

Définition 2.1.4. *On notera $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid (a,b) \in \mathbb{Z}^2\}$ le sous-anneau de $\mathbb{Q}(\sqrt{d})$ engendré par $\sqrt{d}$.*

Pour la suite si $\mathcal{L}/\mathcal{K}$ est une extension et $x \in \mathcal{L}$ on notera $\mu_{x,\mathcal{K}}$ le polynôme minimal de x sur $\mathcal{K}$.
De plus, on parlera de $\mathbb{Q}(\sqrt{d})$ sans préciser que $d \in \mathbb{Z}\backslash\{0,1\}$ est sans facteur carré.
Également, on écrira "soit $z = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$" sans préciser que $(a,b) \in \mathbb{Q}^2$.

Remarque 2.1.2. Le fait que d soit sans facteur carré assure que $\sqrt{d} \notin \mathbb{Q}$.
En effet, par l'absurde supposons que $\sqrt{d} = \frac{p}{q}$ avec $(p,q) \in \mathbb{Z} \times \mathbb{N}^*$ premiers entre eux alors on a : $q^2 d = p^2$ et donc $p^2 \mid dq^2$ mais p^2 et q^2 étant premiers entre eux on a par le lemme de Gauβ $p^2 \mid d$ d'où $p^2 = 1$ et $q^2 d = 1$ donc d est inversible dans $\mathbb{Z}$ et donc $d = -1$ mais $\sqrt{-1} = \pm i \notin \mathbb{Q}$, c'est une contradiction.

Remarque 2.1.3. Soit $z = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ alors on a l'équivalence suivante :

$$z \in \mathbb{Q} \iff b = 0.$$

En effet, on a via la remarque précédente $\mu_{\sqrt{d},\mathbb{Q}} = X^2 - d$ qui est de degré 2 donc $(1, \sqrt{d})$ forme une $\mathbb{Q}$-base de $\mathbb{Q}(\sqrt{d})$.

Remarque 2.1.4. Si d admet un facteur carré il s'écrit $d = k^2 d'$ avec k entier > 1 et $d' \in \mathbb{Z}$, on a $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{d'})$ ce qui permet de se ramener au cas sans facteur carré.

Remarque 2.1.5. Un entier dans $\mathbb{Z}\backslash\{0,1\}$ sans facteur carré s'écrit $d = \pm p_1 ... p_r$ avec les p_i premiers distincts.

Proposition 2.1.2. *Les sous-extensions de $\mathbb{C}/\mathbb{Q}$ de degré 2 sont exactement les corps quadratiques.*

Démonstration. :
Soit $\mathcal{K}/\mathbb{Q}$ une sous-extension de $\mathbb{C}/\mathbb{Q}$ de degré 2 on a donc : $\mathbb{Q} \subsetneq \mathcal{K}$ et donc il existe $x \in \mathcal{K}\backslash\mathbb{Q}$ et nécessairement $\mathbb{Q}(x) = \mathcal{K}$ (par multiplicativité des degrés et l'hypothèse $x \notin \mathbb{Q}$) donc $\deg(\mu_{x,\mathbb{Q}}) = 2$ et donc il existe $(a,b) \in \mathbb{Q}^2$ tels que :

$$x^2 + ax + b = 0$$

et donc si on note $\delta = \frac{p}{q} \in \mathbb{Q}$ le discriminant de $P = X^2 + aX + b$ on a :

$$\mathcal{K} = \mathbb{Q}(x) = \mathbb{Q}(\frac{-a \pm \sqrt{\delta}}{2}) = \mathbb{Q}(\sqrt{\delta}) = \mathbb{Q}(\sqrt{\frac{p}{q}}) = \mathbb{Q}(\sqrt{pq})$$

et on peut supposer que pq est sans facteur carré via la remarque 2.1.4. □

2.1.2 Conjugaison, trace, norme

Définition 2.1.5 (Groupe de Galois). *Soit $\mathcal{L}/\mathcal{K}$ une extension, on appelle groupe de Galois de $\mathcal{L}$ sur $\mathcal{K}$, Gal($\mathcal{L}/\mathcal{K}$) l'ensemble des automorphismes (de corps) de $\mathcal{L}$ laissant invariant $\mathcal{K}$ point par point.*

Proposition 2.1.3. *L'application conjugaison définie par :*

$$\sigma : \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}(\sqrt{d})$$

$$z = a + b\sqrt{d} \mapsto \overline{z} = a - b\sqrt{d}$$

est un automorphisme de corps.
De plus, $Gal(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) = \{Id, \sigma\}$.

Démonstration. :
Soit $i : \mathbb{Q} \to \mathbb{Q}(\sqrt{d})$ l'inclusion et $\phi \in \text{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$ alors on peut voir ϕ comme un prolongement de i, or $\mu_{\sqrt{d},\mathbb{Q}} = X^2 - d$ et $i(\mu_{\sqrt{d},\mathbb{Q}}) = \mu_{\sqrt{d},\mathbb{Q}}$ et possède donc deux racines $\sqrt{d}$ et $-\sqrt{d}$ et donc par le théorème de prolongement des isomorphismes on a deux possibilités pour ϕ soit $\phi(\sqrt{d}) = \sqrt{d}$ et $\phi = Id$ ou $\phi(\sqrt{d}) = -\sqrt{d}$ et $\phi = \sigma$. De plus, $\sigma \circ \sigma = Id$ donc σ est bijective. □

Remarque 2.1.6. Dans le cas $d < 0$ la conjugaison coïncide avec la conjugaison complexe.

Remarque 2.1.7. L'anneau $\mathbb{Z}[\sqrt{d}]$ est stable par σ.

Définition 2.1.6 (Trace)**.** *Soit* $z = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$*, on définit la trace de* z *par la formule :*

$$Tr(z) = z + \overline{z} = 2a \in \mathbb{Q}$$

Définition 2.1.7 (Norme)**.** *Soit* $z = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$*, on définit la norme de* z *par la formule :*

$$N(z) = z\overline{z} = a^2 - db^2 \in \mathbb{Q}$$

Remarque 2.1.8. Dans le cas $d < 0$ on a $N(z) = |z|^2$.

Proposition 2.1.4. *La trace est additive et la norme multiplicative.*

Lemme 2.1.1. *Soit* $z = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$.
Le polynôme minimal de z *sur* $\mathbb{Q}$ *est* $X - z$ *si* $z \in \mathbb{Q}$ *et sinon c'est* $X^2 - Tr(z)X + N(z) = (X - z)(X - \overline{z})$.

Démonstration. :
Si $z \in \mathbb{Q}$ il est clair que $\mu_{z,\mathbb{Q}} = X - z$.
Si $z \notin \mathbb{Q}$ alors $P = X^2 - Tr(z)X + N(z) \in \mathbb{Q}[X]$ et vérifie $P(z) = 0$ de plus, il est de degré 2 donc il est irréductible sur $\mathbb{Q}$ si et seulement si il n'a pas de racines dans $\mathbb{Q}$, or les racines de P sont z et $\overline{z}$ qui ne sont pas dans $\mathbb{Q}$ donc nécessairement $\mu_{z,\mathbb{Q}} = X^2 - Tr(z)X + N(z)$. □

Lemme 2.1.2. *Soit* $z \in \mathbb{Q}(\sqrt{d})$ *alors :*

$$z \text{ est entier sur } \mathbb{Z} \iff (Tr(z), N(z)) \in \mathbb{Z}^2.$$

Démonstration. :
$\boxed{\Longleftarrow}$: Découle directement du lemme 2.2.1.
$\boxed{\Longrightarrow}$: Soit $z \in \mathbb{Q}(\sqrt{d})$ entier sur $\mathbb{Z}$.
Si $z \in \mathbb{Q}$ comme $\mathbb{Z}$ est factoriel on a par la proposition 15 que $z \in \mathbb{Z}$ et donc $(Tr(z), N(z)) \in \mathbb{Z}^2$.
Si $z \notin \mathbb{Q}$ comme z est entier sur $\mathbb{Z}$, il existe $P \in \mathbb{Z}[X]$ unitaire non nul tel que $P(z) = 0$ et comme $\mathbb{Z}[X]$ est factoriel on peut supposer P irréductible sur $\mathbb{Z}$ mais alors comme P est unitaire il est primitif et donc par le théorème de Gauβ, P est irréductible sur $\mathbb{Q}$ et donc $P = \mu_{z,\mathbb{Q}} = X^2 - Tr(z)X + N(z) \in \mathbb{Z}[X]$ d'où le résultat. □

2.1.3 L'anneau des entiers

Théorème 2.1.1. *Si on note $\mathcal{A}_d$ l'anneau des entiers de $\mathbb{Q}(\sqrt{d})$ alors on a :*
$\mathcal{A}_d = \mathbb{Z}[\sqrt{d}]$ *si* $d \equiv 2$ *ou* 3 $[4]$
$\mathcal{A}_d = \mathbb{Z}[\frac{1+\sqrt{d}}{2}] = \{a + b(\frac{1+\sqrt{d}}{2}) \mid (a,b) \in \mathbb{Z}^2\}$ *si* $d \equiv 1$ $[4]$

Pour toute la suite, $\mathcal{A}_d$ désignera l'anneau des entiers de $\mathbb{Q}(\sqrt{d})$.

Remarque 2.1.9. Le cas $d \equiv 0$ $[4]$ est exclu puisque d est supposé sans facteur carré.

Remarque 2.1.10. On a : $\mathbb{Z}[\sqrt{d}] \subset \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$.
En effet, si on note $\alpha_d = \frac{1+\sqrt{d}}{2}$ alors $-1 + 2\alpha_d = \sqrt{d}$ d'où l'inclusion.

Pour la suite on notera $\alpha_d = \frac{1+\sqrt{d}}{2}$.

Remarque 2.1.11. Si $d \equiv 1$ $[4]$ on a :

$$(Tr(\alpha_d), N(\alpha_d)) = (1, \frac{1-d}{4}) \in \mathbb{Z}^2$$

et donc α_d est entier sur $\mathbb{Z}$ et donc $\mathbb{Z}[\alpha_d] \subset \mathcal{A}_d$.
Ainsi, les anneaux proposés sont bien entiers sur $\mathbb{Z}$.

Démonstration. :
Soit $z = a + b\sqrt{d} \in \mathcal{A}_d$ donc par le lemme 2.1.2 $(Tr(z), N(z)) = (2a, a^2 - db^2) \in \mathbb{Z}^2$, on distingue alors deux cas :
1) $a \in \mathbb{Z}$: Alors dans ce cas $db^2 \in \mathbb{Z}$. Soit alors $(p,q) \in \mathbb{Z} \times \mathbb{N}^*$ tels que $b = \frac{p}{q}$ et p et q soient premiers entre eux, on a $d\frac{p^2}{q^2} \in \mathbb{Z}$ donc $q^2 \mid dp^2$ et par le lemme de Gauβ, $q^2 \mid d$ mais d est supposé sans facteur carré donc $q = 1$ et donc $b = p \in \mathbb{Z}$ et finalement $z \in \mathbb{Z}[\sqrt{d}]$.
2) $a \notin \mathbb{Z}$: Alors dans ce cas $a = \frac{a'}{2}$ avec $a' \in \mathbb{Z}$ impair. On écrit de nouveau $b = \frac{p}{q}$ et alors $n = N(z) = \frac{a'^2}{4} - d\frac{p^2}{q^2} \in \mathbb{Z}$ donc :

$$4q^2n = a'^2q^2 - 4dp^2 \ (\spadesuit)$$

d'où $4 \mid a'^2q^2$ mais a' étant impair, on a $4 \mid q^2$ et donc q est pair soit alors q' tel que $q = 2q'$ et $(\spadesuit)$ se réécrit alors :

$$4q'^2n = a'^2q'^2 - dp^2 \ (\spadesuit)$$

d'où $q'^2 \mid dp^2$ donc $q'^2 \mid d$ et alors $q' = 1$, et $(\spadesuit)$ devient :

$$4n = a'^2 - dp^2 \ (\spadesuit).$$

Par suite comme $q = 2$ et p et q sont premiers entre eux on a p impair. Ainsi a' et p étant tous deux impairs leur carré est congru à 1 modulo 4 et en passant $(\spadesuit)$ modulo 4 on trouve :

$$0 \equiv 1 - d \ [4]$$

ou encore :

$$d \equiv 1 \ [4].$$

Ainsi le deuxième cas ne se produit que lorsque $d \equiv 1$ $[4]$, achevant alors la démonstration pour les cas $d \equiv 2$ ou 3 $[4]$.
On suppose donc $d \equiv 1$ $[4]$, le calcul précédent montre alors que :

$$z = \frac{a'}{2} + \frac{p}{2}\sqrt{d}$$

avec a' et p impairs, et au final :

$$z = \alpha_d + \frac{a'-1}{2} + \frac{p-1}{2}\sqrt{d} = \alpha_d + \frac{a'-1}{2} + \frac{p-1}{2}(-1 + 2\alpha_d) \in \mathbb{Z}[\alpha_d].$$

□

Proposition 2.1.5. *Les anneaux $\mathcal{A}_d$ sont de Dedekind.*

Démonstration. :
Du fait que $\mathbb{Z}$ soit de dimension 1 on a par la proposition 1.3.4 que l'anneau $\mathcal{A}_d$ est de dimension 1.
Le caractère intégralement clos a été évoqué dans la remarque 2.1.1.
Il ne reste donc que le caractère noethérien.
Or si $d \equiv 2$ ou 3 $[4]$ alors :

$$\mathcal{A}_d = \mathbb{Z}[\sqrt{d}] \simeq \mathbb{Z}[X]/(X^2 - d)$$

et donc comme $\mathbb{Z}$ est noethérien car principal on a en vertu du théorème de la base de Hilbert que $\mathbb{Z}[X]$ est noethérien et donc $\mathbb{Z}[\sqrt{d}] \simeq \mathbb{Z}[X]/(X^2 - d)$ est noethérien par la proposition 1.3.3.
Si $d \equiv 1$ $[4]$ alors :

$$\mathcal{A}_d = \mathbb{Z}[\frac{1+\sqrt{d}}{2}] \simeq \mathbb{Z}[X]/(X^2 - X + \frac{1-d}{4})$$

et on conclut de la même manière qu'avant. □

Remarque 2.1.12. [Preuve des isomorphismes cités précédemment] Montrons d'abord que pour $d \equiv 2$ ou 3 $[4]$:

$$\mathcal{A}_d = \mathbb{Z}[\sqrt{d}] \simeq \mathbb{Z}[X]/(X^2 - d)$$

pour cela on considère le morphisme d'évaluation :

$$ev_{\sqrt{d}} : \mathbb{Z}[X] \to \mathbb{C}$$

$$P \mapsto P(\sqrt{d}).$$

Il est clair que $(X^2 - d) \subset Ker(ev_{\sqrt{d}})$ montrons l'inclusion réciproque, soit $P \in Ker(ev_{\sqrt{d}})$, $X^2 - d$ étant à coefficient dominant inversible on peut réaliser la division euclidienne de P par $X^2 - d$ dans $\mathbb{Z}[X]$ soit alors $(Q, R) \in \mathbb{Z}[X]^2$ tels que :

$$P = Q(X^2 - d) + R \text{ et } \deg(R) \leq 1$$

alors en composant par $ev_{\sqrt{d}}$ on obtient :

$$0 = ev_{\sqrt{d}}(P) = ev_{\sqrt{d}}(Q(X^2 - d) + R) = 0 + ev_{\sqrt{d}}(R) = R(\sqrt{d})$$

mais R étant de degré au plus 1 et $\mu_{\sqrt{d},\mathbb{Q}} = X^2 - d$ (lemme 2.1.1) nécessairement $R = 0$ et donc $P \in (X^2 - d)$.
De plus on a par définition que $Im(ev_{\sqrt{d}}) = \mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid (a, b) \in \mathbb{Z}^2\}$ (la dernière égalité découlant également d'une division euclidienne par $X^2 - d$). Le premier théorème d'isomorphisme nous donne alors l'isomorphisme souhaité.
Si $d \equiv 1$ $[4]$ on a alors $X^2 - X + \frac{1-d}{4} \in \mathbb{Z}[X]$ et on fait comme ce qui précède en considérant cette fois :

$$ev_{\frac{1+\sqrt{d}}{2}} : \mathbb{Z}[X] \to \mathbb{C}$$

$$P \mapsto P(\frac{1+\sqrt{d}}{2}).$$

2.2 Les corps quadratiques imaginaires

2.2.1 Les corps quadratiques imaginaires

Définition 2.2.1. *On appelle corps quadratique imaginaire tout corps quadratique $\mathbb{Q}(\sqrt{d})$ avec $d < 0$ (et sans facteur carré).*

Remarque 2.2.1. Si $d < 0$ en notant $q = -d$ on a alors : $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(i\sqrt{q})$.

Pour toute la suite, on adopte désormais les conventions suivantes, on note $\mathcal{K}_q = \mathbb{Q}(i\sqrt{q})$ avec q comme précédemment sans préciser que $q > 0$ est sans facteur carré. On note également $\alpha_q = \frac{1+i\sqrt{q}}{2}$ et $\mathcal{A}_q$ l'anneau des entiers de $\mathcal{K}_q$ (donc $\mathbb{Z}[i\sqrt{q}]$ ou $\mathbb{Z}[\alpha_q]$).

Remarque 2.2.2. Ainsi on a précédemment montré que :
$\mathcal{A}_q = \mathbb{Z}[i\sqrt{q}]$ si $-q \equiv 2$ ou 3 $[4]$ et $\mathcal{A}_q = \mathbb{Z}[\alpha_q]$ si $-q \equiv 1$ $[4]$ donc : $\mathcal{A}_q = \mathbb{Z}[i\sqrt{q}]$ si $q \equiv 2$ ou 1 $[4]$ et $\mathcal{A}_q = \mathbb{Z}[\alpha_q]$ si $q \equiv 3$ $[4]$. (attention au changement de congruence dû au fait que l'on a posé $q = -d$)
Si $z = a + bi\sqrt{q} \in \mathbb{Z}[i\sqrt{q}]$ on a $(Tr(z), N(z)) = (2a, a^2 + qb^2)$ (un changement de signe a de nouveau lieu) et si $z = a + b\alpha_q \in \mathbb{Z}[\alpha_q]$ on a $(Tr(z), N(z)) = (2a + b, ab + a^2 + \frac{b^2(q+1)}{4})$.
On rappelle également que : $\mathbb{Z}[i\sqrt{q}] \simeq \mathbb{Z}[X]/(X^2 + q)$ et $\mathbb{Z}[\alpha_q] \simeq \mathbb{Z}[X]/(X^2 - X + \frac{1+q}{4})$ (si $q \equiv 3$ $[4]$) .

Remarque 2.2.3. On a $\mathcal{A}_3 = \mathbb{Z}[\alpha_3] = \mathbb{Z}[\alpha_3 - 1] = \mathbb{Z}[j]$ où $j = e^{\frac{2i\pi}{3}}$.

Remarque 2.2.4. Le résultat suivant nous servira souvent pour la suite : si $n \in \mathbb{Z}$ divise $z = a + bi\sqrt{q}$ dans $\mathbb{Z}[i\sqrt{q}]$ (ou $z = a + b\alpha_q$ dans $\mathbb{Z}[\alpha_q]$) alors n divise a et b dans $\mathbb{Z}$.

2.2.2 Étude des éléments des anneaux quadratiques imaginaires

Lemme 2.2.1. *Soit $z \in \mathcal{A}_q$ alors, $N(z) \in \mathbb{N}$ et $N(z) = 0$ si et seulement si $z = 0$.*

Démonstration. :
On rappelle qu'on a vu en remarque 2.1.8 que pour les corps quadratiques imaginaires on a : $N(z) = z\overline{z} = |z|^2$ or on observe par la remarque 2.2.2 que si $z \in \mathcal{A}_q$ alors $N(z) \in \mathbb{Z}$ d'où le résultat. □

Lemme 2.2.2. *Soit $z = a + bi\sqrt{q} \in \mathbb{Z}[i\sqrt{q}]$ avec $b \neq 0$ alors :*

$$N(z) \geq q \text{ et } N(z) = q \iff z = \pm i\sqrt{q}.$$

Démonstration. :
Si $b \neq 0$ alors :

$$N(z) = a^2 + qb^2 \geq qb^2$$

(car $a^2 \geq 0$) et donc :

$$N(z) \geq q$$

(car $b^2 \geq 1$ car $b \neq 0$).
De plus, les inégalités précédentes sont des égalités si et seulement si $a^2 = 0$ et $b^2 = 1$ donc si et seulement si $(a, b) = (0, \pm 1)$ donc si et seulement si $z = \pm i\sqrt{q}$. □

Lemme 2.2.3. *(On suppose $q \equiv 3$ $[4]$). Soit $z = a + b\alpha_q \in \mathbb{Z}[\alpha_q]$ avec $b \neq 0$ alors :*

$$N(z) \geq \frac{q+1}{4} \text{ et } (N(z) = \frac{q+1}{4} \iff z = \pm\alpha_q \text{ ou } z = \pm\overline{\alpha_q} = \pm(1 - \alpha_q)).$$

Démonstration. :
On a $N(z) = N(a + b\alpha_q) = a^2 + ab + \frac{b^2(q+1)}{4} = (a + \frac{b}{2})^2 + \frac{qb^2}{4} \geq \frac{q}{4}$.
Mais $N(z) \in \mathbb{N}$, et si on écrit $q = 4k + 3$ avec $k \in \mathbb{N}$ alors par ce qui précède : $N(z) \geq k + \frac{3}{4}$. D'où $N(z) \geq k + 1 = \frac{q+1}{4}$.
On s'intéresse maintenant à l'équation $N(z) = \frac{q+1}{4}$.
Premièrement, si $|b| \geq 2$ alors $N(z) \geq q > \frac{q+1}{4}$ donc pour avoir le cas d'égalité il faut nécessairement que $|b| = 1$.
Si $b = 1$ alors on est amené à résoudre $(a + \frac{1}{2})^2 + \frac{q}{4} = \frac{q+1}{4}$ donc à résoudre : $(a + \frac{1}{2})^2 = \frac{1}{4}$ donc on cherche a tel que $|(a + \frac{1}{2})| = \frac{1}{2}$, à savoir $a = 0$ ou $a = -1$.
Si $b = -1$ alors on est amené à résoudre $(a + \frac{-1}{2})^2 + \frac{q}{4} = \frac{q+1}{4}$ donc à résoudre : $(a + \frac{-1}{2})^2 = \frac{1}{4}$ donc on cherche a tel que $|(a + \frac{-1}{2})| = \frac{1}{2}$ à savoir $a = 0$ ou $a = 1$. □

Pour la suite si $\mathcal{A}$ est un anneau on note $\mathcal{A}^\times$ l'ensemble des éléments inversibles de $\mathcal{A}$.

Lemme 2.2.4. *Soit $z \in \mathcal{A}_q$ alors, $z \in \mathcal{A}_q^\times \iff N(z) = 1$.*

Démonstration. :
$\boxed{\implies}$: Soit $z \in \mathcal{A}_q^\times$ alors il existe $u \in \mathcal{A}_q$ tel que $1 = zu$ mais alors par multiplicativité de la norme on a :

$$N(1) = 1 = N(zu) = N(z)N(u)$$

et donc comme $(N(u), N(z)) \in \mathbb{N}^2$ on a par l'équation précédente $N(z) \in \mathbb{Z}^\times \cap \mathbb{N} = \{1\}$ donc $N(z) = 1$.
$\boxed{\impliedby}$: Soit $z \in \mathcal{A}_q$ tel que $N(z) = 1$ alors :

$$1 = N(z) = z\overline{z}$$

et comme $\overline{z} \in \mathcal{A}_q$, z est inversible d'inverse $\overline{z}$. □

Proposition 2.2.1. *On a les égalités suivantes :*
$\mathcal{A}_1^\times = \mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$
$\mathcal{A}_3^\times = \mathbb{Z}[j]^\times = \{\pm 1, \pm j, \pm j^2\}$
Pour $q > 0$, $q \neq 1$, $q \neq 3$, $\mathcal{A}_q^\times = \{\pm 1\}$

Démonstration. :
D'après le lemme 2.2.4 pour trouver les inversibles de $\mathcal{A}_q$ il suffit de résoudre l'équation $N(z) = 1$ d'inconnue $z \in \mathcal{A}_q$.
Si $q \equiv 2$ ou 1 [4] :
Si $q = 1$ soit $z = a + bi \in \mathcal{A}_1$ alors en vertu du lemme 2.2.2 si $b \neq 0$ on a $N(z) = q = 1$ si et seulement si $z = \pm i$ et si $b = 0$ alors $N(z) = a^2$ et $a^2 = 1 \iff a = \pm 1$.
Et ainsi $\mathcal{A}_1^\times = \{\pm 1, \pm i\}$.
Si $q > 1$ soit $z = a + bi\sqrt{q} \in \mathcal{A}_q$ alors en vertu du lemme 2.2.2 nécessairement $b = 0$ et donc $z = a$ et $N(z) = a^2 = 1$ et $z = \pm 1$.
Si $q \equiv 3$ [4] :
Si $q = 3$ soit $z = a + bj \in \mathcal{A}_3$ alors en vertu du lemme 2.2.3 si $b \neq 0$ on a $N(z) = \frac{q+1}{4} = 1$ si et seulement si $z = \pm\overline{j}$ ou $\pm(1 + \overline{j})$ donc si et seulement si $z = \pm j, \pm j^2$. Si $b = 0$ alors $z = a$ et $N(z) = a^2 = 1$ et $z = \pm 1$.
Et ainsi $\mathcal{A}_3^\times = \{\pm 1, \pm j, \pm j^2\}$.
Si $q > 3$ soit $z = a + b\alpha_q \in \mathcal{A}_q$ alors en vertu du lemme 2.2.3 nécessairement $b = 0$ et donc $z = a$ et $N(z) = a^2 = 1$ et donc $z = \pm 1$. □

Proposition 2.2.2. *Soit $p \in \mathbb{N}$ un nombre premier, alors :*

p est réductible dans $\mathcal{A}_q$ si et seulement si il existe $z \in \mathcal{A}_q$ tel que $N(z) = p$

Démonstration. :
$\boxed{\implies}$: Soit p un nombre premier réductible dans $\mathcal{A}_q$ comme p est toujours non nul et non inversible car $N(p) = p^2 > 1$ si il est réductible c'est qu'il existe $(u, v) \in \mathcal{A}_q^2$ tels que $p = uv$ avec u et v non inversibles mais alors :

$$N(p) = p^2 = N(u)N(v)$$

et $N(u) > 1$ et $N(v) > 1$ donc comme p est premier nécessairement $N(u) = N(v) = p$.
$\boxed{\impliedby}$: Soit $z \in \mathcal{A}_q$ tel que $N(z) = p$ alors :

$$N(z) = z\overline{z} = p$$

et z et $\overline{z}$ sont non inversibles dans $\mathcal{A}_q$ car $N(z) = N(\overline{z}) = p > 1$; donc p est réductible. □

2.2.3 Détermination d'anneaux quadratiques imaginaires non principaux

Lemme 2.2.5. *Si $q \equiv 1$ ou 2 $[4]$ et $q > 2$ alors 2 est irréductible dans $\mathcal{A}_q$.*

Démonstration. :
En effet, par l'absurde supposons que 2 soit réductible dans $\mathcal{A}_q$ alors par la proposition 2.2.2 il existe $z = a + ib\sqrt{q} \in \mathcal{A}_q = \mathbb{Z}[i\sqrt{q}]$ (on est dans le cas $q \equiv 1$ ou 2 $[4]$) tel que $N(z) = 2$. Or si $b \neq 0$ en vertu du lemme 2.2.2, $N(z) \geq q > 2$ donc nécessairement $b = 0$ et donc $N(z) = a^2 = 2$ ce qui est absurde car l'équation $a^2 = 2$ ne possède pas de solutions dans $\mathbb{Z}$. □

Lemme 2.2.6. *Si $q \equiv 3$ $[4]$ et $q > 7$ alors 2 est irréductible dans $\mathcal{A}_q$.*

Démonstration. :
C'est la même démonstration que précédemment mais en utilisant le lemme 2.2.3. □

Proposition 2.2.3. *Si $q \equiv 1$ ou 2 $[4]$ et $q > 2$ alors $\mathcal{A}_q$ n'est pas principal.*

Démonstration. :
Il suffit de montrer que $\mathcal{A}_q$ n'est pas factoriel.
Montrons que $\mathcal{A}_q$ ne vérifie pas le lemme d'Euclide : d'après le lemme précédent 2 est irréductible dans $\mathcal{A}_q$.
Montrons alors que 2 n'est pas premier dans $\mathcal{A}_q$:
On a :

$$q^2 + q \equiv 0 \ [2]$$

donc $2 \mid q^2 + q$ mais on a aussi :

$$q^2 + q = (q + i\sqrt{q})(q - i\sqrt{q})$$

mais $2 \nmid (q + i\sqrt{q})$ et $2 \nmid (q - i\sqrt{q})$ (remarque 2.2.4). □

Proposition 2.2.4. *Si $q \equiv 7$ $[8]$ et $q > 7$ alors $\mathcal{A}_q$ n'est pas principal.*

Démonstration. :
D'abord $q \equiv 7$ $[8]$ $\implies$ $q \equiv 3$ $[4]$ donc $\mathcal{A}_q = \mathbb{Z}[\alpha_q]$, l'idée est la même que précédemment on va montrer que 2 n'est pas premier en montrant que (2) n'est pas premier, et pour cela on s'intéresse à $\mathcal{A}_q/(2)$.
On a rappelé précédemment que $\mathbb{Z}[\alpha_q] \simeq \mathbb{Z}[X]/(X^2 - X + \frac{1+q}{4})$ donc :

$$\mathcal{A}_q/(2) \simeq \mathbb{Z}[X]/(X^2 - X + \frac{1+q}{4}, 2) \simeq \mathbb{F}_2[X]/(X^2 - X + \frac{1+q}{4}).$$

Soit alors $k \in \mathbb{N}$ tel que $q = 8k + 7$ on a $P = X^2 - X + \frac{1+q}{4} = X^2 - X + 2k + 2$ et donc si on réduit modulo 2 :

$$\overline{P} = X^2 - X = X(X - 1)$$

est réductible sur $\mathbb{F}_2$ donc $(X(X-1))$ n'est pas premier donc $\mathbb{F}_2[X]/(X^2 - X + \frac{1+q}{4})$ n'est pas intègre donc $\mathcal{A}_q/(2)$ ne l'est pas non plus donc 2 n'est pas premier dans $\mathcal{A}_q$. □

Remarque 2.2.5. :
Si $q \equiv 3$ $[8]$ on ne peut pas faire de même car (2) est premier non nul dans ce cas-là. En effet, si on écrit $q = 8k + 3$ avec $k \in \mathbb{Z}$ alors $P = X^2 - X + \frac{q+1}{4} = X^2 - X + 2k + 1$ et ainsi après réduction modulo 2, $\overline{P} = X^2 + X + 1$ est irréductible sur $\mathbb{F}_2$.

Lemme 2.2.7. *Soit $q \geq 15$, alors $\sqrt{q} < \frac{q+1}{4}$.*

Démonstration. :
On s'intéresse à la fonction polynomiale $f : x \mapsto x^2 - 4x + 1$ alors f possède deux racines $2 - \sqrt{3}$ et $2 + \sqrt{3}$ et $2 + \sqrt{3} < \sqrt{15}$. Ainsi comme $\sqrt{q} \geq 15$, $f(\sqrt{q}) > 0$. □

Proposition 2.2.5. *Si q est composé et $q > 1$ alors $\mathcal{A}_q$ n'est pas principal.*

Démonstration. :
On peut supposer $q \equiv 3$ [4] (les autres cas ont été éliminés dans la proposition 2.2.3) de plus 3, 7 et 11 étant premiers on peut supposer $q \geq 15$. Du fait que q est composé il admet un facteur premier $p \in \mathbb{N}$ tel que $1 < p \leq \sqrt{q} < \frac{q+1}{4}$ (lemme 2.2.7) ainsi en combinant la proposition 2.2.2 et le lemme 2.2.3, p est irréductible (car p premier) dans $\mathcal{A}_q$. Montrons alors que p n'est pas premier dans $\mathcal{A}_q$:
On a $p \mid (2\alpha_q - 1)^2 = -q$ mais $p \nmid (2\alpha_q - 1)$. (remarque 2.2.4) □

2.2.4 Détermination des anneaux quadratiques imaginaires euclidiens

Lemme 2.2.8. *Soit $\mathcal{A}$ un anneau euclidien, alors il existe $z \in \mathcal{A}$ non inversible, tel que :*

$$\pi : \mathcal{A}^\times \cup \{0\} \to \mathcal{A}/(z) \text{ soit surjective.}$$

Où $\pi : a \mapsto [a]$ est la projection canonique.

Démonstration. :
Si $\mathcal{A}$ est un corps, $z = 0$ convient.
Si $\mathcal{A}$ n'est pas un corps, on note δ un stathme sur $\mathcal{A}$ et alors :

$$E = \{\delta(x) \mid x \neq 0, x \text{ non inversible}\}$$

est un sous-ensemble de $\mathbb{N}$ non vide donc il admet un minimum ; on choisit alors $z \neq 0$ et non inversible tel que $\delta(z)$ soit minimal dans E. Soit alors $a \in \mathcal{A}$ et $(q, r) \in \mathcal{A}^2$ tels que $a = qz + r$ avec $\delta(r) < \delta(z)$ ou $r = 0$.
Ainsi :

$$[r] = [a].$$

Si $r \neq 0$ alors r est inversible sans quoi il contredirait la minimalité de $\delta(z)$ et donc $r \in \mathcal{A}^\times \cup \{0\}$ est un antécédent de a par π ; et si $r = 0$ alors c'est aussi un antécédent qui convient.
Ainsi la restriction de π est bien surjective. □

Lemme 2.2.9. *Soit $q > 0$ et $z \in \mathcal{A}_q$, $z \neq 0$ alors (z) est d'indice fini dans $\mathcal{A}_q$ et :*

$$[\mathcal{A}_q : (z)] = N(z)$$

Démonstration. :
Pour cette preuve on identifie $\mathbb{C}$ avec $\mathbb{R}^2$ on commence par remarquer que :

$$\mathcal{A}_q = \mathbb{Z}[\beta_q] = \Lambda((1, \beta_q))$$

(définition 1.2.4) avec $\beta_q = \alpha_q$ ou $i\sqrt{q}$ et donc en particulier $\mathcal{A}_q$ est un réseau de $\mathbb{C}$ (proposition 1.2.3).
Or :

$$(z) = z\mathcal{A}_q = \Lambda((z, z\beta_q))$$

est également un réseau donc en tant que sous-groupe de $\mathcal{A}_q$ donc il est d'indice fini et (proposition 1.2.9) :

$$[\mathcal{A}_q : (z)] = \frac{\text{covol}(z\mathcal{A}_q)}{\text{covol}(\mathcal{A}_q)}.$$

D'autre part, l'application :

$$\varphi : \mathbb{C} \simeq \mathbb{R}^2 \to \mathbb{C} \simeq \mathbb{R}^2$$
$$\omega = (x, y) \mapsto z\omega = \begin{pmatrix} Re(z) & -Im(z) \\ Im(z) & Re(z) \end{pmatrix} (x \ y)^T$$

est une application linéaire, ainsi si $X \subset \mathbb{C}$ est une partie mesurable on a :

$$\mu(\varphi(X)) = \left|\det(\begin{pmatrix} Re(z) & -Im(z) \\ Im(z) & Re(z) \end{pmatrix})\right| \mu(X) = N(z)\mu(X).$$

En particulier :

$$[\mathcal{A}_q : (z)] = \frac{\text{covol}(z\mathcal{A}_q)}{\text{covol}(\mathcal{A}_q)} = N(z).$$

□

Proposition 2.2.6. *Si $q \neq 1, 2, 3, 7, 11$ alors $\mathcal{A}_q$ n'est pas euclidien.*

Démonstration. :
On peut supposer $q \equiv 3$ [4] en vertu de la proposition 2.2.3 et on peut même supposer $q \equiv 3$ [8] en vertu de la proposition 2.2.4 ainsi comme $q \equiv 3$ [8] et $q > 11$ on a $q \geq 19$.
Par l'absurde supposons que $\mathcal{A}_q$ soit euclidien alors d'après le lemme 2.2.8 il existerait $z \in \mathcal{A}_q$ non inversible tel que :

$$|\mathcal{A}_q/(z)| \leq |\mathcal{A}_q^\times \cup \{0\}| = |\{-1, 1, 0\}| = 3.$$

(proposition 2.2.1) Autrement dit (lemme 2.2.9) il existerait $z \in \mathcal{A}_q$ non inversible tel que :

$$N(z) \leq 3$$

mais si $z \in \mathbb{Z}$ alors $N(z) = z^2 \geq 4$ (car $z \neq \pm 1$ car non inversible) donc nécessairement $z \in \mathcal{A}_q \setminus \mathbb{Z}$. Mais alors le lemme 8 assure que $N(z) \geq \frac{q+1}{4} \geq \frac{19+1}{4} = 5 > 3$ c'est une contradiction. □

Lemme 2.2.10. *Si $q = 1, 2, 3, 7$ ou 11 alors pour tout $z \in \mathbb{C}$ il existe $t \in \mathcal{A}_q$ tel que $N(z - t) < 1$.*

Remarque 2.2.6. On peut parler de la norme de $z - t$ même si $z - t \notin \mathcal{K}_q$ car (remarque 2.1.8) $z \mapsto |z|^2$ est parfaitement définie sur $\mathbb{C}$.

Démonstration. :
Premier cas : $q = 1$ ou 2 :
On écrit $z = x + iy$ avec $(x, y) \in \mathbb{R}^2$ soit alors a et b des entiers les plus proches de x et $\frac{y}{\sqrt{q}}$ respectivement (la partie entière ou la partie entière plus un) de sorte que :

$$|x - a| \leq \frac{1}{2}$$

$$|\frac{y}{\sqrt{q}} - b| \leq \frac{1}{2}.$$

Considérons alors $t = a + ib\sqrt{q} \in \mathcal{A}_q$, on a :

$$N(z - t) = (x - a)^2 + (y - b\sqrt{q})^2 = (x - a)^2 + q(\frac{y}{\sqrt{q}} - b)^2 \leq \frac{q+1}{4} < 1$$

(la dernière inégalité repose sur le fait que $q \leq 2$) et cela conclut ce premier cas.
Deuxième cas : $q = 3, 7$ ou 11 :
On écrit $z = x + y\alpha_q$ avec $(x, y) \in \mathbb{R}^2$ soit alors a un entier le plus proche de y et b un entier le plus proche de $x + \frac{y-a}{2}$ de sorte que :

$$|y - a| \leq \frac{1}{2}$$

$$|x + \frac{y - a}{2} - b| \leq \frac{1}{2}.$$

Considérons alors $t = b + \alpha_q a \in \mathcal{A}_q$, on a :

$$N(z - t) = (x - b + \frac{y - a}{2})^2 + q\frac{(y - a)^2}{4}$$

$$\leq \frac{1}{4} + \frac{q}{16} \leq \frac{q + 4}{16} \leq \frac{15}{16} < 1$$

et cela conclut le deuxième cas. □

Théorème 2.2.1. *Si $q = 1, 2, 3, 7$ ou 11 alors $\mathcal{A}_q$ est euclidien.*

Démonstration. :
On va montrer que l'anneau est euclidien relativement à la norme. On suppose donc $q = 1, 2, 3, 7$ ou 11, soient $z, w \in \mathcal{A}_q \setminus \{0\}$ d'après le lemme 2.2.10 il existe $t \in \mathcal{A}_q$ tel que $N(\frac{z}{w} - t) < 1$.
Posons alors $r = z - tw = w(\frac{z}{w} - t) \in \mathcal{A}_q$ et on a :

$$N(r) = N(w)N(\frac{z}{w} - t) < N(w)$$

et par construction $z = tw + r$.

□

2.3 Retour sur les anneaux non principaux

2.3.1 Nouvelle détermination d'anneaux non principaux

Théorème 2.3.1. *Si $q < 10\ 000$ et $q \neq 1, 2, 3, 7, 11, 19, 43, 67$ et 163, alors $\mathcal{A}_q$ n'est pas principal.*

Remarque 2.3.1. Stark et Heegner ont prouvé en 1967 que les neuf anneaux cités précédemment sont en fait les seuls anneaux quadratiques imaginaires principaux. On pourra consulter : A complete determination of the complex quadratic fields of class-number one, Michigan Math. J. 14 (1967), pp.1-27.

Démonstration. :
En combinant les propositions 2.2.5, 2.2.4 et 2.2.3 on peut supposer que q est premier sans facteur carré et $q \equiv 3$ [8] ainsi si on suppose $q < 10\ 000$ et $q \neq 1, 2, 3, 7, 11, 19, 43, 67$ et 163 il s'agit de prouver que $\mathcal{A}_q$ n'est pas principal pour :
$q \in \{59, 83, 107, 131, 139, 179, 211, 227, 251, 283, 307, 331, 347, 379, 419, 443, 467, 491, 499, 523, 547, 563, 571, 587, 619, 643, 659, 683, 691, 739, 787, 811, 827, 859, 883, 907, 947, 971, 1019, 1051, 1091, 1123, 1163, 1171, 1187, 1259, 1283, 1291, 1307, 1427, 1451, 1459, 1483, 1499, 1523, 1531, 1571, 1579, 1619, 1627, 1667, 1699, 1723, 1747, 1787, 1811, 1867, 1907, 1931, 1979, 1987, 2003, 2011, 2027, 2083, 2099, 2131, 2179, 2203, 2243, 2251, 2267, 2339, 2347, 2371, 2411, 2459, 2467, 2531, 2539, 2579, 2659, 2683, 2699, 2707, 2731, 2803, 2819, 2843, 2851, 2939, 2963, 2971, 3011, 3019, 3067, 3083, 3163, 3187, 3203, 3251, 3259, 3299, 3307, 3323, 3331, 3347, 3371, 3467, 3491, 3499, 3539, 3547, 3571, 3643, 3659, 3691, 3739, 3779, 3803, 3851, 3907, 3923, 3931, 3947, 4003, 4019, 4027, 4051, 4091, 4099, 4139, 4211, 4219, 4243, 4259, 4283, 4339, 4363, 4451, 4483, 4507, 4523, 4547, 4603, 4643, 4651, 4691, 4723, 4787, 4931, 4987, 5003, 5011, 5051, 5059, 5099, 5107, 5147, 5171, 5179, 5227, 5323, 5347, 5387, 5419, 5443, 5483, 5507, 5531, 5563, 5651, 5659, 5683, 5779, 5827, 5843, 5851, 5867, 5923, 5939, 5987, 6011, 6043, 6067, 6091, 6131, 6163, 6203, 6211, 6299, 6323, 6379, 6427, 6451, 6491, 6547, 6563, 6571, 6619, 6659, 6691, 6763, 6779, 6803, 6827, 6883, 6899, 6907, 6947, 6971, 7019, 7027, 7043, 7187, 7211, 7219, 7243, 7283, 7307, 7331, 7411, 7451, 7459, 7499, 7507, 7523, 7547, 7603, 7643, 7691, 7699, 7723, 7867, 7883, 7907, 7963, 8011, 8059, 8123, 8147, 8171, 8179, 8219, 8243, 8291, 8363, 8387, 8419, 8443, 8467, 8539, 8563, 8627, 8699, 8707, 8731, 8747, 8779, 8803, 8819, 8867, 8923, 8963, 8971, 9011, 9043, 9059, 9067, 9091, 9187, 9203, 9227, 9283, 9323, 9371, 9403, 9419, 9467, 9491, 9539, 9547, 9587, 9619, 9643, 9739, 9787, 9803, 9811, 9851, 9859, 9883, 9907, 9923, 9931\}$.
Pour cela on va montrer que pour ces valeurs $\mathcal{A}_q$ n'est pas factoriel en appliquant la recette suivante : on sait que si p est un nombre premier $< \frac{q+1}{4}$ alors il est irréductible dans $\mathcal{A}_q$ (lemme 2.2.3 et proposition 2.2.2) ainsi si on veut prouver que (p) n'est pas premier on utilise le fait que :

$$\mathcal{A}_q/(p) \simeq \mathbb{F}_p[X]/(X^2 - X + \frac{q+1}{4}).$$

Et alors, si $p > 2$ il suffit de montrer que $P = X^2 - X + \frac{q+1}{4}$ est réductible sur $\mathbb{F}_p$ or le discriminant de P est $-q$ et P étant de degré 2 il suffit ainsi de prouver que $-q$ est un carré modulo p. On obtient donc la recette suivante pour éliminer nos candidats potentiels :
Étape 1 : On choisit un nombre premier $p > 2$
Étape 2 : On regarde les carrés modulo p et enlève de notre liste tous les $q > 4p - 1$ tels que $-q$ est un carré modulo p.
$\boxed{p = 3}$ est irréductible pour $q > 11$ et $-q$ est un carré modulo 3 si et seulement si $-q$ est congru à 0 ou 1 modulo 3. On peut donc éliminer 59, 83, 107, 131, 179, 227, 251, 347, 419, 443, 467, 491, 563, 587, 659, 683, 827, 947, 971, 1019, 1091, 1163, 1187, 1259, 1283, 1307, 1427, 1451, 1499, 1523, 1571, 1619, 1667, 1787, 1811, 1907, 1931, 1979, 2003, 2027, 2099, 2243, 2267, 2339, 2411, 2459, 2531, 2579, 2699, 2819, 2843, 2939, 2963, 3011, 3083, 3203, 3251, 3299, 3323, 3347, 3371, 3467, 3491, 3539, 3659, 3779, 3803, 3851, 3923, 3947, 4019, 4091, 4139, 4211, 4259, 4283, 4451, 4523, 4547, 4643, 4691, 4787, 4931, 5003, 5051, 5099, 5147, 5171, 5387, 5483, 5507, 5531, 5651, 5843, 5867, 5939, 5987, 6011, 6131, 6203, 6299, 6323, 6491, 6563, 6659, 6779, 6803, 6827, 6899, 6947, 6971, 7019, 7043, 7187, 7211, 7283, 7307, 7331, 7451, 7499, 7523, 7547, 7643, 7691, 7883, 7907, 8123, 8147, 8171, 8219, 8243, 8291, 8363, 8387, 8627, 8699, 8747, 8819, 8867, 8963, 9011, 9059, 9203, 9227, 9323, 9371, 9419, 9467, 9491, 9539, 9587, 9803, 9851 et 9923.
$\boxed{p = 5}$ est irréductible pour $q > 19$ et $-q$ est un carré modulo 5 si et seulement si $-q$ est congru à $0, 1$ ou 4 modulo 5. On peut donc éliminer 139, 211, 331, 379, 499, 571, 619, 691, 739, 811, 859, 1051, 1171, 1291, 1459, 1531, 1579, 1699, 2011, 2131, 2179, 2251, 2371, 2539, 2659, 2731, 2851, 2971, 3019, 3259, 3331, 3499, 3571, 3691, 3739, 3931, 4051, 4099, 4219, 4339, 4651, 5011, 5059, 5179, 5419, 5659, 5779, 5851, 6091, 6211, 6379, 6451, 6571, 6619, 6691, 7219, 7411, 7459, 7699, 8011, 8059, 8179, 8419, 8539, 8731, 8779, 8971, 9091, 9619, 9739, 9811, 9859 et 9931.
$\boxed{p = 7}$ est irréductible pour $q > 27$ et $-q$ est un carré modulo 7 si et seulement si $-q$ est congru à $0, 1, 2$ ou 4

modulo 7. On peut donc éliminer 283, 307, 523, 643, 787, 1123, 1483, 1627, 1867, 1987, 2203, 2467, 2707, 2803, 3163, 3307, 3547, 3643, 4003, 4483, 4507, 4723, 4987, 5227, 5323, 5347, 5563, 5683, 5827, 6067, 6163, 6907, 7027, 7243, 7507, 7867, 8707, 8923, 9043, 9187, 9547 et 9883.
$p = 11$ est irréductible pour $q > 43$ et $-q$ est un carré modulo 11 si et seulement si $-q$ est congru à $0, 1, 3, 4, 5$ ou 9 modulo 11. On peut donc éliminer 547, 1723, 2683, 3187, 3907, 4243, 4363, 6547, 6883, 7603, 7963, 8443, 8467, 9283, 9643, 9787, 9907.
$\boxed{p = 13}$ est irréductible pour $q > 51$ et $-q$ est un carré modulo 13 si et seulement si $-q$ est congru à $0, 1, 3, 4, 9, 10$ ou 12 modulo 13. On peut donc éliminer 883, 907, 2083, 3067, 4027, 4603, 5443, 6763, 7723, 8563 et 9403.
$p = 17$ est irréductible pour $q > 67$ et $-q$ est un carré modulo 17 si et seulement si $-q$ est congru à $0, 1, 2, 4, 8, 9, 13, 15$ ou 16 modulo 17. On peut donc éliminer 1747, 2347, 6043 et 6427.
$\boxed{p = 19}$ est irréductible pour $q > 75$ et $-q$ est un carré modulo 19 si et seulement si $-q$ est congru à $0, 1, 4, 5, 6, 7, 9, 11, 16$ ou 17 modulo 19. On peut donc éliminer 5107 et 5923.
$\boxed{p = 23}$ est irréductible pour $q > 91$ et $-q$ est un carré modulo 23 si et seulement si $-q$ est congru à $0, 1, 2, 3, 4, 6, 8, 9, 12, 13, 16$ ou 18 modulo 23. On peut donc éliminer 8803 et 9067.
Tous les candidats ayant été éliminés cela conclut. □

On trouvera en annexe le programme python utilisé pour cette démonstration.

Remarque 2.3.2. Lorsqu'on teste si $-q$ est un carré modulo p, on aurait pu enlever 0 de la liste des carrés car q est supposé premier.

Remarque 2.3.3. Avec la même technique en allant jusqu'à $p = 37$ on peut prouver le même résultat pour $q < 100\ 000$.

Remarque 2.3.4. Avec la même technique en allant jusqu'à $p = 37$ et $q < 1\ 000\ 000$ il reste 3 candidats : 222643, 253507 et 991027. Si on monte jusqu'à $p = 43$ les 3 candidats se font éliminer.

Remarque 2.3.5. Si on laisse $19, 43, 67$ et 163 dans la liste des candidats ils ne se font jamais éliminer pour $p \leq 1000$. On en déduit ainsi que :
- 3 est premier dans $\mathcal{A}_{19}$
- 3 et 5 sont premiers dans $\mathcal{A}_{43}$
- $3, 5, 7$ et 13 sont premiers dans $\mathcal{A}_{67}$
- $3, 5, 7, 13, 19$ et 23 sont premiers dans $\mathcal{A}_{163}$.

(Si ça n'avait pas été le cas ils auraient été éliminés)

2.3.2 Nouvelle détermination d'anneaux principaux

On propose dans cette sous-section de déterminer une condition suffisante sur $\mathcal{A}_q$ pour que celui-ci soit principal. Pour toute la suite on note $\mathbb{P}$ l'ensemble des nombres premiers (dans $\mathbb{N}$).

Lemme 2.3.1. *Soit $p \in \mathbb{P}$, il existe à isomorphisme près un unique anneau de cardinal p, qui est $\mathbb{Z}/p\mathbb{Z}$.*

Démonstration. :
Soit A un anneau de cardinal p et φ le morphisme naturel de $\mathbb{Z}$ dans A, A étant fini φ n'est pas injectif donc son noyau est de la forme $c\mathbb{Z}$ avec $c \neq 0$ et par le premier théorème d'isomorphisme A contient un sous-anneau isomorphe à $\mathbb{Z}/c\mathbb{Z} \simeq Im(\varphi) \subset A$. Donc en particulier $\mathbb{Z}/c\mathbb{Z}$ est un sous-groupe de $(A, +)$ mais ce groupe étant de cardinal p et $c \neq 0$ nécessairement $c = p$ et donc $Im(\varphi) \simeq \mathbb{Z}/p\mathbb{Z}$ et ainsi $A \simeq \mathbb{Z}/p\mathbb{Z}$. □

Définition 2.3.1. *Soit $C \geq 1$ et $q > 0$ sans facteur carré on dira que C est une q-borne si :*

$$\forall p \in \mathbb{P},\ \mathcal{A}_q/(p) \text{ non intègre} \implies \exists k \in \mathbb{Z},\ 1 \leq k \leq C \text{ tel que } kp \text{ soit une norme dans } \mathcal{A}_q.$$

Définition 2.3.2. *Soit $C \geq 2$ et $q > 0$ sans facteur carré on dira que C est q-adaptée si :*

$$\forall p \in \mathbb{P},\ p \leq C \implies p \text{ est premier dans } \mathcal{A}_q.$$

Définition 2.3.3 (Condition (*))**.** *Soit $q > 0$ sans facteur carré on dira que q vérifie la condition (*) si il existe $C \geq 2$ tel que C soit une q-borne et est q-adaptée.*

Remarque 2.3.6. Soit $q > 0$ sans facteur carré alors 1 est une q-borne signifie en formulant la contraposée :

$$\forall p \in \mathbb{P},\ p \text{ n'est pas une norme dans } \mathcal{A}_q \implies (p) \text{ est premier dans } \mathcal{A}_q.$$

Et donc par la proposition 2.2.2 :

$$\forall p \in \mathbb{P},\ p \text{ est irréductible dans } \mathcal{A}_q \implies (p) \text{ est premier dans } \mathcal{A}_q.$$

Proposition 2.3.1. *Soit $q > 0$ sans facteur carré si q vérifie la condition (*) alors 1 est une q-borne.*

Démonstration. :
Soit $C \geq 2$ tel que C soit une q-borne et q-adaptée.
Soit $p \in \mathbb{P}$ tel que $\mathcal{A}_q/(p)$ ne soit pas intègre, montrons que p est une norme dans $\mathcal{A}_q$. Comme C est q-adaptée nécessairement $p > C$. De plus, C est une q-borne donc il existe $1 \leq k \leq C$ tel que kp soit une norme dans $\mathcal{A}_q$. On note k_0 le plus petit k qui convient et $z \in \mathcal{A}_q$ tel que $N(z) = k_0 p$. On a donc :

$$k_0 p = N(z) = z\overline{z}. \ (\heartsuit)$$

On souhaite montrer que $k_0 = 1$. Par l'absurde supposons $k_0 \neq 1$. Soit alors p_0 un facteur premier de k_0 ; on a en particulier $p_0 \leq C$ donc comme C est q-adaptée, p_0 est premier dans $\mathcal{A}_q$ donc par ($\heartsuit$), $p_0 \mid z$ ou $p_0 \mid \overline{z}$ et dans les deux cas $p_0 \mid z$ (remarque 2.2.4). Soit donc $w \in \mathcal{A}_q$ tel que :

$$z = wp_0. \ (\spadesuit)$$

On a en particulier :

$$\overline{z} = \overline{w}p_0. \ (\spadesuit)$$

Soit également $k' \in \mathbb{N}$ tel que $k_0 = k'p_0$, on a donc en injectant ($\spadesuit$) dans ($\heartsuit$) :

$$k'p_0 p = w\overline{w}p_0^2.$$

Autrement dit :

$$k'p = w\overline{w}p_0 = N(w)p_0. \ (\clubsuit)$$

On arrive à une équation dans $\mathbb{N}$ mais du fait que $p > C$ et $p_0 \leq C$ et qu'ils sont tous les deux premiers (dans $\mathbb{N}$) on a que $p_0 \nmid p$ donc par ($\clubsuit$) et le lemme de Gauβ, $p_0 \mid k'$. Soit donc $k'' \in \mathbb{N}$ tel que $k' = p_0 k''$ on a alors en injectant dans ($\clubsuit$) :

$$k''p = N(w)$$

avec $1 \leq k'' < k_0$ (car $k'' < k' < k_0$ car $p_0 > 1$) contredisant alors la minimalité de k_0. Donc $k_0 = 1$ et $k_0 p = p$ est une norme dans $\mathcal{A}_q$. □

Proposition 2.3.2. *Soit $q > 3$ sans facteur carré si 1 est une q-borne alors les irréductibles de $\mathcal{A}_q$ sont, au signe près :*
les $p \in \mathbb{P}$ premiers (dans $\mathbb{N}$), qui ne sont pas des normes dans $\mathcal{A}_q$.
les $z \in \mathcal{A}_q$ tels que $N(z) \in \mathbb{P}$.
et ces irréductibles sont tous premiers dans $\mathcal{A}_q$.

Démonstration. :
Montrons dans un premier temps que nos candidats sont effectivement irréductibles et même premiers.
Soit $z \in \mathcal{A}_q$ et $p \in \mathbb{P}$ tel que $N(z) = p$ alors par le lemme 2.2.9 :

$$|\mathcal{A}_q/(z)| = N(z) = p.$$

Donc par le lemme 2.3.1, $\mathcal{A}_q/(z) \simeq \mathbb{Z}/p\mathbb{Z}$ est intègre donc (z) est premier (non nul) donc z est premier donc irréductible dans $\mathcal{A}_q$.
Le cas des nombres premiers dans $\mathbb{N}$ découle de la proposition 2.2.2 et de la remarque 2.3.6.
On considère maintenant $z \in \mathcal{A}_q$ irréductible, soit p un facteur premier (dans $\mathbb{N}$) de $N(z)$.

Premier cas : p est irréductible dans $\mathcal{A}_q$ alors par la remarque 2.3.6 l'idéal (p) est premier. Or $p \mid N(z) = z\overline{z}$ donc $p \mid z$ ou $p \mid \overline{z}$ et dans les deux cas $p \mid z$ (remarque 2.2.4). Du fait que z est irréductible et que p est non inversible alors nécessairement $z = \pm p$ (proposition 2.2.1).
Deuxième cas : p est réductible et donc il existe $w \in \mathcal{A}_q$ tel que $N(w) = p$ (proposition 2.2.2) et alors comme précédemment (w) est premier non nul donc w est premier et $w \mid N(z) = z\overline{z}$ donc $w \mid z$ ou $w \mid \overline{z}$ (or si z est irréductible dans $\mathcal{A}_q$ alors $\overline{z}$ aussi en tant qu'image de z par l'automorphisme de conjugaison) donc $w = \pm z$ ou $w = \pm\overline{z}$ et donc $N(z) = N(\overline{z}) = N(w) = p$. □

Corollaire 2.3.1. *Soit $q > 0$ sans facteur carré si q vérifie la condition (*) alors $\mathcal{A}_q$ est principal.*

Démonstration. :
Par les propositions 2.1.5 et 1.3.5, il suffit de montrer que l'anneau $\mathcal{A}_q$ est factoriel, pour cela il suffit de montrer que $\mathcal{A}_q$ vérifie le lemme d'Euclide (corollaire 1.3.3). Or si q vérifie la condition (*) par la proposition 2.3.1 q est compatible avec 1 et ainsi par la proposition 2.3.2 on connaît tous les irréductibles de $\mathcal{A}_q$ et ils sont tous premiers dans $\mathcal{A}_q$. Donc $\mathcal{A}_q$ vérifie le lemme d'Euclide. □

2.3.3 19,43,67 et 163 vérifient la condition (*)

On propose dans cette sous-section de montrer que si $q \in \{19, 43, 67, 163\}$ alors $\mathcal{A}_q$ est principal. On propose pour cela deux méthodes, une qui utilise le théorème de Minkowski (théorème 1.2.3) et une qui utilise le principe des tiroirs de Dirichlet.

Proposition 2.3.3. *Soit $p \in \mathbb{P}$ et $q \equiv 3$ [4], alors :*
Si $\mathcal{A}_q/(p)$ n'est pas intègre alors il existe $z \in \mathcal{A}_q \setminus \mathbb{Z}$ et $\lambda \in \mathbb{N}^*$ tel que $N(z) = \lambda p$. De plus, on peut supposer que $z = -u + \alpha_q$ avec $u \in \mathbb{Z}$. De plus on peut choisir u tel que $|u| \leq \frac{p-1}{2}$.

Démonstration. :
On a l'isomorphisme (comme $q \equiv 3$ [4]) :

$$\mathcal{A}_q/(p) \simeq \mathbb{F}_p[X]/(X^2 - X + \frac{q+1}{4}).$$

Donc si $\mathcal{A}_q/(p)$ n'est pas intègre nécessairement $P = X^2 - X + \frac{q+1}{4}$ n'est pas irréductible sur $\mathbb{F}_p$ donc P admet une racine $\overline{u}$ dans $\mathbb{F}_p$. Ainsi $u^2 - u + \frac{q+1}{4} = \lambda p$ pour un $\lambda \in \mathbb{Z}$ et un $u \in \mathbb{Z}$, or $u^2 - u + \frac{q+1}{4} = N(-u + \alpha_q)$ (remarque 2.2.2) donc :

$$N(-u + \alpha_q) = \lambda p.$$

Et donc nécessairement $\lambda \in \mathbb{N}^*$ (car $-u + \alpha_q \neq 0$). De plus si p est impair $\{\frac{1-p}{2}, ..., -1, 0, 1, ..., \frac{p-1}{2}\}$ est un ensemble de représentants de $\mathbb{F}_p$ donc on peut choisir u de sorte que $|u| \leq \frac{p-1}{2}$.
Si $p = 2$ et $q \equiv 3$ [8] alors au vu de la remarque 2.2.5, (2) est premier et donc le résultat reste vrai et si $q \equiv 7$ [8] on peut prendre $u = 0$. □

La preuve de Minkowski

Notation 2.3.1. *Soit $q \in \mathbb{N}^*$ pour toute la suite on note $M_q = \frac{2\sqrt{q}}{\pi}$.*

On propose de montrer que si $q \in \{19, 43, 67, 163\}$ alors M_q est une q-borne et est q-adaptée. Le fait que M_q soit une q-borne nécessite seulement l'hypothèse $q \equiv 3$ [4].

Proposition 2.3.4. *Soit $q \equiv 3$ [4] alors M_q est une q-borne.*

Démonstration. :
Soit $p \in \mathbb{P}$ tel que $\mathcal{A}_q/(p)$ ne soit pas intègre. Par la proposition 2.3.3 il existe $z = -u + \alpha_q$ avec $u \in \mathbb{Z}$ tel que $N(z) = \lambda p$ avec $\lambda \in \mathbb{N}^*$.
Considérons :

$$L = \{a + b\alpha_q \in \mathcal{A}_q \mid (a, b) \in \mathbb{Z}^2, a + bu \equiv 0\ [p]\}.$$

Alors $L = \Lambda((p, -u + \alpha_q))$ (définition 1.2.4) est un réseau de $\mathbb{C}$ et L est un sous-groupe de $(\mathcal{A}_q, +)$ dont tous les éléments ont une norme multiple de p.

En effet, soit $x = a + b\alpha_q \in L$ alors $x = a + b(\alpha_q - u + u) = a + bu + b(\alpha_q - u)$ or $x \in L$ donc il existe $r \in \mathbb{Z}$ tel que $a + bu = rp$ et donc $x = rp + b(\alpha_q - u) \in \Lambda((p, -u + \alpha_q))$. L'inclusion réciproque $\Lambda((p, -u + \alpha_q)) \subset L$ est claire. De plus :

$$\begin{aligned} N(x) &= N(rp + b(\alpha_q - u)) = N(rp - bu + b\alpha_q) \\ &= (rp - bu)b + (rp - bu)^2 + \frac{b^2(q+1)}{4} \\ &= rpb - b^2u + r^2p^2 - 2brpu + b^2u^2 + \frac{b^2(q+1)}{4} \\ &= rpb + r^2p^2 - 2brpu + b^2(u^2 - u + \frac{(q+1)}{4}) \\ &= rpb + r^2p^2 - 2brpu + b^2N(-u + \alpha_q) \\ &= rpb + r^2p^2 - 2brpu + b^2\lambda p \in p\mathbb{Z}. \end{aligned}$$

On a alors $\text{covol}(L) = \left|\det(\begin{pmatrix} \frac{\sqrt{q}}{2} & 0 \\ -u + \frac{1}{2} & p \end{pmatrix})\right| = p\frac{\sqrt{q}}{2}$.
Or la boule (euclidienne) fermée $C = B(0, \sqrt{pM_q}) = \{z \in \mathbb{C} \mid |z| \leq \sqrt{pM_q}\}$ est une partie mesurable convexe symétrique compacte et $\mu(C) = 2p\sqrt{q}$ donc :

$$\frac{\mu(C)}{2^2} = \text{covol}(L).$$

Donc d'après le théorème de Minkowski (théorème 1.2.3) il existe $z \neq 0$ dans $L \cap C$. Donc il existe $k \in \mathbb{N}^*$ tel que $N(z) = kp$ (car $z \in L$) et de plus $z \in C$ donc $kp = N(z) = |z|^2 \leq pM_q$ et donc $1 \leq k \leq M_q$. □

Proposition 2.3.5. *Soit $q \in \{19, 43, 67, 163\}$ alors M_q est q-adaptée.*

Démonstration. :
On a $M_q = \frac{2\sqrt{q}}{\pi} \approx 0.636\sqrt{q}$. Ainsi pour $q = 19, 43, 67, 163$ on a respectivement $M_q \approx 2.77, 4.17, 5.21, 8.12$ et les p à tester sont respectivement 2 ; $2, 3$; $2, 3, 5$; $2, 3, 5, 7$ on renvoie alors vers les remarques 2.3.5 et 2.2.5. □

Ainsi en combinant les propositions 2.3.5 et 2.3.4 on obtient :

Corollaire 2.3.2. *Soit $q \in \{19, 43, 67, 163\}$ alors M_q est une q-borne et est q-adaptée. En particulier, q vérifie la condition (*).*

La preuve de Dirichlet

Notation 2.3.2. *Soit $q \in \mathbb{N}^*$ pour toute la suite on note $T_q = \sqrt{\frac{q}{3}}$.*

On propose de montrer que si $q \in \{19, 43, 67, 163\}$ alors T_q est une q-borne et est q-adaptée.

Théorème 2.3.2 (Principe des tiroirs de Dirichlet)**.** *Soit $k \in \mathbb{N}^*$ et $n \in \mathbb{N}$ tel que $n > k$. Soit X un ensemble à n éléments et Y un ensemble à k éléments alors il n'existe pas d'application injective de X dans Y.*

Lemme 2.3.2 (Lemme d'approximation des réels)**.** *Soit $v \in \mathbb{R}$ (resp. $v \in \mathbb{R} \setminus \mathbb{Q}$), soit $l \in \mathbb{N}$, $l \geq 2$. Il existe $k \in \mathbb{N}$ tel que $1 \leq k \leq l - 1$ et $n \in \mathbb{Z}$ tels que :*

$$|kv - n| \leq \frac{1}{l} \text{ (resp. } <).$$

Démonstration. :
On note pour tout $i \in [[0, l-1]]$, $v_i = iv - \lfloor iv \rfloor$ et $v_l = 1$. On considère ensuite pour $j \in [[0, l-2]]$, $T_j = [\frac{j}{l}, \frac{j+1}{l}[$ et $T_{l-1} = [\frac{l-1}{l}, 1]$.
Soit maintenant $\varphi : \{0, ..., l\} \to \{T_0, ..., T_{l-1}\}$ qui à i associe l'unique T_j tel que $v_i \in T_j$. (φ est bien définie car pour tout i, $v_i \in [0, 1]$ et $[0, 1] = \sqcup_{j \in [[0, l-1]]} T_j$.)

Alors $|\{0,...,l\}| = l+1 > l = |\{T_0,...,T_{l-1}\}|$ donc par le principe des tiroirs de Dirichlet, φ n'est pas injective. Ainsi, il existe $j \in [[0, l-1]]$ tel que T_j ait au moins deux antécédents. On distingue alors trois cas.
Premier cas : T_0 a au moins deux antécédents, comme $\varphi(0) = T_0$ et $\varphi(l) = T_{l-1} \neq T_0$ c'est qu'il existe $k \in [[1, l-1]]$ tel que $\varphi(k) = T_0$ et donc $v_k \in T_0$ et $|v_k| < \frac{1}{l}$ d'où :

$$|kv - \lfloor kv \rfloor| < \frac{1}{l}.$$

Deuxième cas : T_{l-1} a au moins deux antécédents, comme $\varphi(0) = T_0$ et $\varphi(l) = T_{l-1} \neq T_0$ c'est qu'il existe $k \in [[1, l-1]]$ tel que $\varphi(k) = T_{l-1}$ et donc $v_k \in T_{l-1}$ et $|v_k - 1| \leq \frac{1}{l}$ d'où :

$$|kv - \lfloor kv \rfloor - 1| \leq \frac{1}{l}.$$

(et si $v \notin \mathbb{Q}$ on ne peut pas avoir égalité)
Troisième cas : Il existe $j \in [[1, l-2]]$ tel que T_j ait au moins deux antécédents, comme $\varphi(0) = T_0 \neq T_j$ et $\varphi(l) = T_{l-1} \neq T_j$ c'est qu'il existe i_1 et i_2 dans $[[1, l-1]]$ avec $i_1 < i_2$ tels que $\varphi(i_1) = \varphi(i_2)$ et donc :

$$|i_1 v - \lfloor i_1 v \rfloor - (i_2 v - \lfloor i_2 v \rfloor)| < \frac{1}{l}$$

autrement dit :

$$|(i_1 - i_2)v - \lfloor i_1 v \rfloor + \lfloor i_2 v \rfloor| < \frac{1}{l}.$$

□

Pour rappel, on note $\mathcal{K}_q = \mathbb{Q}(i\sqrt{q})$.

Lemme 2.3.3. *Soit $q \equiv 3$ [4] sans facteur carré, soit $l \in \mathbb{N}^*$ tel que $l > T_q$. Soit $x \in \mathcal{K}_q$ alors il existe $k \in \mathbb{N}$, tel que $1 \leq k \leq l-1$ et $d \in \mathcal{A}_q$ tels que $N(kx - d) < 1$.*

Démonstration. :
On écrit $x = a + bi\sqrt{q} \in \mathcal{K}_q$ donc $x = a + b(2\alpha_q - 1) = a' + b'\alpha_q$ (avec $(a', b') \in \mathbb{Q}^2$). En remarquant que $T_q \geq 1$, d'après le lemme d'approximation des réels il existe $k \in \mathbb{N}$ tel que $1 \leq k \leq l-1$ et $n \in \mathbb{Z}$ tels que $|kb' - n| \leq \frac{1}{l}$.
On a alors :

$$kx = ka' + kb'\alpha_q = ka' + \frac{kb'}{2} + i\frac{kb'}{2}\sqrt{q}.$$

On choisit ensuite un entier m tel que :

$$|ka' + \frac{kb'}{2} - \frac{n}{2} - m| \leq \frac{1}{2}.$$

Posons $d = m + n\alpha_q \in \mathcal{A}_q$ de sorte que :

$$N(kx - d) = (ka' + k\frac{b'}{2} - \frac{n}{2} - m)^2 + \frac{(kb' - n)^2 q}{4} \leq \frac{1}{4} + \frac{q}{4l^2} = \frac{q + l^2}{4l^2} < 1$$

car $l > T_q = \sqrt{\frac{q}{3}}$ d'où $q < 3l^2$. □

Lemme 2.3.4 (Pseudo-division euclidienne)**.** *Avec les notations du lemme 2.3.3. Soit z et w dans $\mathcal{A}_q$, avec $w \neq 0$ alors il existe $k \in \mathbb{N}$ tel que $1 \leq k \leq l-1$ et d et r dans $\mathcal{A}_q$ tels que :*

$$kz = dw + r \text{ et } N(r) < N(w).$$

Démonstration. :
On considère $x = \frac{z}{w} \in \mathcal{K}_q$ ainsi par la lemme 2.3.3 il existe $k \in \mathbb{N}$ tel que $1 \leq k \leq l-1$ et $d \in \mathcal{A}_q$ tels que $N(kx - d) < 1$. Posons $r = kz - dw \in \mathcal{A}_q$ on a donc :

$$N(kx - d) = N(k\frac{z}{w} - d) = N(\frac{1}{w}(kz - dw)) = N(\frac{1}{w})N(kz - dw) = N(\frac{1}{w})N(r) < 1$$

autrement dit : $N(r) < N(w)$ et par construction $kz = dw + r$. □

Proposition 2.3.6. *Soit $q \equiv 3$ [4] tel que T_q soit q-adaptée alors T_q est une q-borne.*

Démonstration. :
Soit $p \in \mathbb{P}$ tel que $\mathcal{A}_q/(p)$ ne soit pas intègre. Par la proposition 2.2.3 il existe $u \in \mathbb{Z},\ \lambda \in \mathbb{N}^*$ tels que $|u| \leq \frac{p-1}{2}$ et $N(-u+\alpha_q) = \lambda p$. Mais T_q est q-adaptée nécessairement $p > T_q$. Donc $3p^2 > q$ et par conséquent :

$$\lambda p = N(-u+\alpha_q) = u^2 - u + \frac{q+1}{4} \leq \frac{(p-1)^2}{4} + \frac{p-1}{2} + \frac{q+1}{4} = \frac{p^2+q}{4} < p^2.$$

D'où : $\lambda < p$. On choisit alors un $z \in \mathcal{A}_q$ vérifiant $N(z) = \lambda p$ tel que λ soit non nul et minimal. Si $\lambda \leq T_q$ il n'y a rien à faire. Sinon par le lemme 2.3.4 on peut effectuer la pseudo-division euclidienne de p par z (on choisit l tel que $0 < l - T_q \leq 1$). Il existe $k \in \mathbb{N}$ tel que $1 \leq k \leq T_q$ et $d, r \in \mathcal{A}_q$ tels que $kp = dz + r$ et $N(r) < N(z)$. Mais alors $N(r)$ est un multiple de p.
En effet si on écrit $dz = a + b\alpha_q \in \mathcal{A}_q$ on a :

$$\begin{aligned} N(r) = N(kp - dz) &= N(kp - a - b\alpha_q) \\ &= k^2p^2 - 2akp - bkp + N(dz) \\ &= p(k^2p - 2ak - bk) + N(d)N(z) \\ &= p(k^2p - 2ak - bk + \lambda N(d)) \in p\mathbb{Z}. \end{aligned}$$

Donc par minimalité de λ on a $N(r) = 0$ et $r = 0$. Ainsi $kp = dz$, d'où :

$$k^2p^2 = N(d)N(z) = N(d)\lambda p \ (\clubsuit)$$

et en divisant par p :

$$k^2p = N(d)\lambda.$$

Or $\lambda < p$ et $p \in \mathbb{P}$ donc p est premier avec λ donc par le lemme de Gauβ $p \mid N(d)$. Soit $\mu \in \mathbb{N}^*$ tel que $N(d) = \mu p$ on en déduit alors par ($\clubsuit$) :

$$\lambda\mu = k^2.$$

Mais alors comme $k \leq T_q < \lambda$ on a $\mu < k \leq T_q$ et donc T_q est une q-borne. □

Proposition 2.3.7. *Soit $q \in \{19, 43, 67, 163\}$ alors T_q est q-adaptée.*

Démonstration. :
On a vu dans la proposition 2.3.5 que dans ces cas-là M_q est q-adaptée or :

$$M_q \approx 0.636\sqrt{q} \text{ et } T_q \approx 0.577\sqrt{q}.$$

Donc en particulier T_q est q-adaptée. □

On obtient en combinant les propositions 2.3.6 et 2.3.7 :

Corollaire 2.3.3. *Soit $q \in \{19, 43, 67, 163\}$ alors T_q est une q-borne et est q-adaptée. En particulier, q vérifie la condition (*).*

Ainsi qu'on passe par la preuve de Minkowski ou par la preuve de Dirichlet on obtient à l'aide du corollaire 2.3.1 :

Théorème 2.3.3. *Soit $q \in \{19, 43, 67, 163\}$ alors $\mathcal{A}_q$ est principal.*

De plus, par la proposition 2.2.6 on a :

Corollaire 2.3.4. *Soit $q \in \{19, 43, 67, 163\}$ alors $\mathcal{A}_q$ est principal non euclidien.*

2.4 Nombres chanceux d'Euler et nombres de Heegner

2.4.1 Théorème de Rabinowitsch

Définition 2.4.1 (Nombre chanceux d'Euler)**.** *Soit $n \in \mathbb{N} \setminus \{0,1\}$ on dit que n est un nombre chanceux d'Euler si :*
Pour tout $k \in [[0, n-2]]$, $P(k) = k^2 + k + n$ est un nombre premier.

Remarque 2.4.1. On obtient une définition équivalente en remplaçant le polynôme P par $Q = X^2 - X + n$ (en effet $Q(k) = k^2 - k + n = P(k-1)$) et en exigeant que $Q(k)$ soit premier pour tout $k \in [[0, n-1]]$.

Remarque 2.4.2. Une étude simple des variations de Q permet de montrer que :

$$Q(0) = n = Q(1) \leq Q(2) \leq ... \leq Q(n-1) \leq Q(n) = n^2$$

Remarque 2.4.3. En remarquant que $P(-k) = k^2 - k + n = Q(k)$ on en déduit que si n est un nombre chanceux d'Euler alors $P(k)$ est premier pour tout $k \in [[-n+1, n-2]]$ et $Q(k)$ est premier pour tout $k \in [[-n+2, n-1]]$.

Exemple 2.4.1. *Les nombres 2 et 3 sont des nombres chanceux d'Euler.*

Définition 2.4.2 (Nombre de Heegner)**.** *Soit $q \in \mathbb{N}^*$ sans facteur carré on dit que q est un nombre de Heegner si $\mathcal{A}_q$ est principal.*

Remarque 2.4.4. D'après les théorèmes 2.3.2, 2.3.1 et 2.2.1 il existe neuf nombres de Heegner inférieurs à 10 000 : $1, 2, 3, 7, 11, 19, 43, 67$ et 163.

Remarque 2.4.5. Il n'en existe en fait pas d'autre, c'est le théorème de Stark-Heegner (remarque 2.3.1) :

$\mathcal{A}_q$ est principal, si et seulement si, $q \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$.

Lemme 2.4.1. *Pour tout $n > 2$:*

$$T_{4n-1} = \sqrt{\frac{4n-1}{3}} \leq n - 1$$

Démonstration. :
Pour tout $n > 0$ on a $T_{4n-1} \leq n - 1 \iff 0 \leq 3n^2 - 10n + 4$. Or la fonction $f : x \mapsto 3x^2 - 10x + 4$ atteint son minimum en $x_0 = \frac{10}{6} \leq 2$ et croît sur $[x_0, +\infty[$. Et on a : $f(2) = -4 < 0$ et $f(3) = 1 > 0$. □

Théorème 2.4.1 (Théorème de Rabinowitsch)**.** *Soit $n \in \mathbb{N} \setminus \{0,1\}$ tel que $4n-1$ soit sans facteur carré alors on l'équivalence suivante :*

n est un nombre chanceux d'Euler si et seulement si $4n-1$ est un nombre de Heegner.

Démonstration. :
$\boxed{\implies}$: Soit n un nombre chanceux d'Euler tel que $4n-1$ soit sans facteur carré. Si $n = 2$, il s'agit alors de prouver que $\mathcal{A}_7$ est principal, on renvoie vers le théorème 2.3.3. Ainsi on peut supposer $n > 2$. Comme $4n - 1 \equiv 3\ [4]$ il s'agit de prouver que $\mathcal{A}_{4n-1}$ est principal. Par la proposition 2.3.6 et le corollaire 2.3.1 il suffit de prouver que T_{4n-1} est $(4n-1)$-adaptée. On raisonne par l'absurde, soit $p \in \mathbb{P}$ tel que $p \leq T_{4n-1}$ et

$\mathcal{A}_{4n-1}/(p)$ soit non intègre. Ainsi, X^2-X+n admet une racine $\overline{u}$ dans $\mathbb{F}_p$ (preuve de la proposition 2.3.3) mais $\{0,1,2,...,p-2,p-1\}$ étant un ensemble de représentants de $\mathbb{F}_p$ on peut choisir $u \in [[0,p-1]]$ tel que :

$$Q(u) = N(-u+\alpha_q) = u^2 - u + n = \lambda p$$

avec $\lambda \in \mathbb{N}^*$ mais alors on a par le lemme 2.4.1 :

$$0 \leq u \leq p-1 \leq p \leq T_{4n-1} \leq n-1$$

et donc comme n est un nombre chanceux d'Euler par hypothèse on a $Q(u) \in \mathbb{P}$ (remarque 2.4.2) ainsi nécessairement $\lambda = 1$ et $Q(u) = p$. Mais alors (remarque 2.4.2) :

$$Q(0) = n \leq Q(u) = p \leq T_{4n-1} \leq n-1$$

autrement dit : $n \leq n-1$. c'est une contradiction.
$\boxed{\Longleftarrow}$: Soit n tel que $4n-1$ soit un nombre de Heegner montrons que n est un nombre chanceux d'Euler. Soit $k \in [[0,n-2]]$, on a :

$$P(k) = k^2 + k + n = N(k+\alpha_q).$$

Supposons que $P(k)$ soit non premier donc $P(k)$ admet un diviseur premier $p \leq \sqrt{P(k)}$. Donc :

$$p^2 \leq P(k) < (n-1)^2 + (n-1) + n = n^2.$$

Et ainsi $p < n$ donc p est irréductible dans $\mathcal{A}_{4n-1}$ (proposition 2.2.2 et lemme 2.2.3) et donc p est premier dans $\mathcal{A}_{4n-1}$ car $\mathcal{A}_{4n-1}$ est factoriel par hypothèse. Mais alors :

$$p \mid P(k) = N(k+\alpha_q) = (k+\alpha_q)(k+\overline{\alpha_q}).$$

Comme p est premier dans $\mathcal{A}_{4n-1}$ alors $p \mid k+\alpha_q$ ou $p \mid k+\overline{\alpha_q}$ mais donc $p \mid 1$ (remarque 2.2.4) c'est une contradiction. □

Chapitre 3

Annexe

```
from math import *

## Les fonctions auxiliaires

def estsansfacteurcarre(q) :
    if q == 0 or q == 1 :
        return False
    for k in range(2,int(sqrt(q))+2) :
        if q % k**2  == 0  :
            return False
    return True
# Fonction permettant de savoir si q est sans facteur carré

def estpremier(q) :
    if q == 0 or q == 1 :
        return False
    if q == 2 :
        return True
    for k in range(2,int(sqrt(q))+2) :
        if q % k == 0 :
            return False
    return True
#Fonction permettant de savoir si q est un nombre premier


def ZpZ(p) :
    return [i for i in range(p)]
#Renvoie une liste qui modèlise Z/pZ


def carreZpZ(p) :
    return list(set([ (i**2) % p for i in ZpZ(p)]))
#Renvoie la liste des carrés de Z/pZ
```

```
## La démonstration de 2.3.1

def candidats(C) :
    L = [i+1 for i in range(18, C+1) if ((i+1) % 8 == 3
    and estsansfacteurcarre(i+1) and estpremier(i+1))]
    return L
#Renvoie les valeurs de q < C candidates
#pour que Aq soit principal

def elimination(x,C) :
    P = [n for n in range(x) if (estpremier(n) and n>2)]
    #Liste des nombres premiers < x
    L = candidats(C)
    #Liste des candidats
    for p in P :
        E = carreZpZ(p)
        El = []
        #Liste des valeurs éliminées par p
        q = 4*p-1
        #Valeur à partir de laquelle p devient irreductible dans Aq
        j = 0
        while j < len(L) :
            if L[j] > q :
                if (-L[j]%p) in E :
                    El.append(L[j])
                    L.remove(L[j])
                else :
                    j = j+1
            else :
                j = j+1
        print(p,q,E,El)
        print("les","candidats","restants","sont",L)
#Permet de retirer des candidats en testant tous les nombres premiers < x
```

3.1 Références

1. G. Berhuy, Algèbre : le grand combat, Calvage et Mounet, 2020.
2. G. Chenevier, Théorie algébrique des nombres, cours à l'X 2011-2019.
3. D. Perrin, Anneaux d'entiers des corps quadratiques imaginaires.
4. D. Perrin, Pourquoi y a-t-il beaucoup de nombres premiers de la forme $n^2 + n + 41$?
5. D. Perrin, Cours d'algèbre, Ellipses, 1996.
6. P. Ribenboim, My Numbers, My Friends : Popular Lectures on Number, Springer, 2000.
7. P. Samuel, Théorie algébrique des nombres, Hermann, 1997.